CITY, UNIVERSITY OF LONDON

MSc IN CYBER SECURITY

MASTERS PROJECT REPORT

2022

DESIGN AND IMPLEMENTATION OF AN ANTI-STALKING SYSTEM FOR AIRTAGS

Author:

Mr. George Jefferson Arthur ABAIDOO

Supervised by:

Dr. Nikos KOMNINOS

Date of Submission:

2nd October 2022

Declaration of Authorship

By submitting this work, I declare that this work is entirely my own except those parts duly identified and referenced in my submission. It complies with any specified word limits and the requirements and regulations detailed in the assessment instructions and any other relevant programme and module documentation. In submitting this work, I acknowledge that I have read and understood the regulations and code regarding academic misconduct, including that relating to plagiarism, as specified in the Programme Handbook. I also acknowledge that this work will be subject to a variety of checks for academic misconduct.

Signed**: George Jefferson Arthur Abaidoo**

Abstract

The release of Apple's tracking devices, the AirTag, has brought about a wave of increased security and privacy concerns. We present a system that addresses the problem of malicious tracking of people and priceless items with these devices by detecting them and alerting the supposed victim. The system was designed and implemented based on research on Bluetooth Low Energy (BLE) signal behaviour and current research on AirTags and BLE devices in general. A unique identifier capable of distinctly identifying the AirTag was derived in this work. A mechanism for estimating the distance of the AirTag was also achieved with the help of a Linear Regression Model used for estimating the one-metre RSSI of the AirTag. Experiments were carried out to validate how accurate the system was in correctly detecting AirTags. The results showed that the implemented system was very accurate in identifying and detecting AirTags from other BLE devices. This report demonstrates what has been done during the project and the results obtained.

Keywords: AirTag, Identifying Token, Advertising Packet, Measured Power.

Acknowledgement

I would like to thank my supervisor, Dr. Nikos Komninos for his valuable inputs, suggestions and assistance. This project would not have been possible without his aid.

Contents

List of Figures

List of Tables

List of Abbreviations

BLE	Bluetooth Low Energy
UWB	Ultra-Wideband
NFC	Near Field Communication
MSD	Manufacturer Specific Data
NDP	Neighbour Discovery Process
GSM	Global System for Global Communications
DSRC	Dedicated Short-Range Communication
GPS	Global Positioning System

To my whole family, the Yeboah Family and the Ghana Education Trust Fund (GETFund) for their unrelenting support and encouragement.

Chapter 1

Introduction and Objectives

This chapter discusses the aims and objectives of this work. It sheds light on the security concern raised by Apple's AirTags and the accompanying areas of research that we focus on.

1.1 Introduction

As one of the biggest companies leading innovation and technological growth in the world according to a Forbes article by (Ponciano, 2022), Apple Incorporated continue to set high standards each year. They are responsible for the invention of almost all technology considered as a daily requirement in the modern era spanning from all forms of computers, through to watches, television experiences, earphones, tablets, to mobile phones – the iconic iPhone which is the most popular device of theirs.

Together with their MacBooks, iPads, iPods Touch, iMacs, HomePods, Apple TV, Apple Watches and AirPods, users are able to form a seamless network and solid ecosystem of devices through which day-to-day life is experienced. This is possible because these devices communicate with one another through communication services such as Wi-Fi, Bluetooth Technology, Ultra-Wide Band Technology and Near Field Communication (NFC). As of 2022, there are about 1.231 billion iPhones units all over the world, with about 1.8 billion total Apple products in circulation according to (Curry, 2022) and (Warren, 2022). This vast and reliable ecosystem of their devices is one of the main grounds on which Apple leveraged in designing and releasing their "AirTag".

"This is AirTag, the next time your couch eats your keys, your AirTag will find them" (CNN, 2020), Apple declared when announcing the AirTag in April 2020. The AirTag is a tracking device which is used to help users track their personal items such as keys, backpack, or other devices. New AirTags are usually synchronized with a user's iPhone, and with the usage of the Find My app, the user is able to track the location of the AirTag at almost all times, and hence by proxy whatever the AirTag is attached to. As a result, a user can track the location of their wallets, keys, purses, backpacks, medical kits, and other devices as long as the AirTag is attached to it. All this was revealed by (Apple, 2020).

However, because of its powerful tracking capabilities, the AirTag can be used for malicious activities mainly involving the unauthorized tracking of other people and items. This device is relatively small in size and as a result is able to be concealed easily and strategically placed for malicious tracking. The AirTag communicates using Bluetooth Low Energy and Ultra-Wide Band Technology (Apple, 2020). There have been many reported cases of the usage of these devices to track victims' luxury cars, belongings and even their homes unknowingly as reported by (Mac and Hill, 2021) in the New York Times. Such disheartening situations have raised a high concern about the compromising of the security, privacy and the safety of users and the general public following the release of the AirTag.

Apple put in measures to tackle these concerns, but they are not comprehensive enough (Clover et al., 2021). The authors noted of these mechanisms that AirTag plays a sound at a random time within an eight-to-twenty-four-hour window after being separated from its registered owner. The sound is to alert the potential victim of supposed tracking by the AirTag for a malicious user. The time period, about 15 seconds and the sound's volume are relatively short and low respectively, and so are not good enough as a remedy. Furthermore, the counter for the eight-to-twenty-four-hour window restarts anytime the supposed perpetrator comes into contact with the AirTag. Also, this time period is enough time for a malicious attacker to cause damage. Another "defensive" measure by Apple is to give alerts on iPhones if there is a case of suspected stalking, but these alerts are often unreliable and infrequent. For Android, Apple released an application called "Tracker Detect" and it helps these users detect supposed malicious AirTags nearby (Mehrotra, 2021). However, this app too is not sufficient since its scan period is very short and makes the experience very manual.

The AirTag is a Bluetooth Low Energy (BLE) device that broadcasts Bluetooth signals, and though there have been studies that have illustrated that Bluetooth devices can be tracked or passively attacked, modern BLE devices are tricky to be tracked due to techniques such as address randomization. (Becker, Li and Starobinski, 2019).

This study aims at providing a reliable mechanism to detect AirTags and the possibility of stalking using them and informing potential victim timely. The result will hopefully improve on the automatic aspect of detecting potential stalking of AirTags for Android devices.

1.2 Aims

The aim of this project is to design and implement an Android application for anti-stalking of AirTags by detecting potential stalking with AirTags and alerting the user through notification. In designing the detection system, the goal is to leverage the usage of passive attacks on the AirTag, which is a BLE device. This is possible because BLE devices announce their presence during connections using advertising channels, however they use periodic changing random MAC addresses when advertising (Becker, Li and Starobinski, 2019). The necessity and requirement here is to extract and use an Identifying Token or characteristic from the advertising packet that can then be used to universally and distinctively detect AirTags.

1.3 Objectives

Research Question: How do you design and implement an anti-stalking system for AirTags?

Objective 1 – To derive an exclusive Identifying Token of AirTags to be able to uniquely identify the device. This includes understanding how BLE technology works, the various phases and analysing BLE packets. The result will be obtaining a feature that can be used to create a filter in the Android App implementation.

Objective 2 – To design and implement an Android Application using Identifying Token to detect AirTags and alert timely. All this will involve using open-source Bluetooth Low Energy API for Android development to implement an application.

Objective 3 – To test and analyze if the system accurately detects AirTags from other BLE devices. The result will be verifying if the system is a viable mechanism for detecting malicious AirTags and possible stalking scenarios.

1.4 Beneficiaries

With the privacy, safety and security implications of the malicious usage of the AirTag, many users will benefit from improvement in these disciplines aforementioned. It will be advantageous to manufacturers and other App developers involved in the development of anti-stalking schemes. This project will also be beneficial to other researchers looking to explore further work in anti-stalking and tracking using BLE technology.

1.5 Work Plan

The project is divided into four phases. These tasks in these phases and how they are executed are detailed in this section.

1.5.1 Research Phase

The first part of the project involves reviewing current literature, project works and studies on the varying areas that the goals of this project cover. This includes the context on AirTags, BLE Technology, Bluetooth and BLE Tracking, and the Privacy concerns raised by this technology. The ideas for design, implementation and testing will be borne from this research.

1.5.2 Design Phase

This is to be done and completed alongside the research phase, and we build on the literature and studies done on AirTags and BLE devices using the various ideas, information and techniques in the critical context. This provides the basis on which key elements of BLE signals we should focus on, a mechanism on extracting essential information from the AirTag, and a structure for implementing and evaluating the application later in the project process.

1.5.3 Implementation Phase

We carry out an implementation of the proposed designs mapped out in the previous phases using applicable platform and API's. The implemented system is evaluated for its validity in this phase using accuracy metrics.

1.5.4 Results and Documentation Phase

We present the result of our implementation and experimentations performed in the previous phase in this final phase of the project. These results are observed, critically evaluated and discussed extensively, with final conclusions and reflections following them.

1.6 Report Structure

1.6.1 Chapter 2, Context

This chapter extensively discusses the critical context of this project. The current research done on BLE Technology and devices as well as the current dive into AirTags are evaluated in order to provide a solid base for how a system can be designed for anti-stalking of AirTags. We look at the various ways BLE technology is used to track items and people, how the various parts of BLE

technology works, and a deep dive into the known information researched about the AirTag, as well as the privacy concerns all these technologies raise.

1.6.2 Chapter 3, Methods

We present implementation of android app system for detecting BLE devices. Extraction of information from BLE packets of devices to discover an Identifying Token for AirTags is detailed in the methods. We introduce the implementation of a filter for specifically detecting an AirTag, and a mechanism for estimating distance from an AirTag. This chapter also demonstrates the experimentation carried out to validate or invalidate the implemented system and findings.

1.6.3 Chapter 4, Results

We introduce the results of the implementation and experimentation and then explain and contextualize each subsection.

1.6.4 Chapter 5, Discussion

We evaluate the results introduced in Chapter 4 against the objectives declared at the beginning of the project. We discuss the outcome of the implementations and experimentations in comparison with the predictions and conceptual analyses introduced at the outset.

1.6.5 Chapter 6, Evaluation, Conclusion, Future Work

We take into consideration the whole end result of the project by reflecting on the successes, failures and the potential for further future work to supplement and enhance this research given more time and resources.

1.6.6 Appendices

Appendix A – Research Proposal Document

Appendix B - Complete sets of Raw Results from Experimentation

Appendix C – Overall Codes

1.7 Contributions

In this project, we present a distinct Identifying Token from the advertising Bluetooth packet of the AirTag which can be used to identify and detect all AirTags.

1.8 Summary

Chapter 1 has covered the general scope of this work. The research work and processes proceeding build on the foundation laid by the background and problem questions introduced. Key areas and their relevance to BLE and AirTag detection are outlined, as well as the beneficiaries, if this project has a successful outcome.

Chapter 2

Context

Chapter 2 touches on Bluetooth and BLE and their current usage and applications in tracking. The privacy concerns raised as a result of this technology is presented. The current information known about the AirTag are also extensively discussed and presented. This chapter sets up the context for the design, implementation, testing and contribution of the project which are illustrated in subsequent chapters.

2.1 BLE Overview

BLE which stands for Bluetooth Low Energy is a subset of the classic Bluetooth and it is a form of wireless communication designed for low power of operation (Bluetooth Technology Website, 2022) and relatively short range of communication. As a result, it is utilized by many developers to build products that meet the requirements of low power for operation (Riyas, 2022). This operating mode enables devices that use this technology to have long battery life. BLE is designed to operate in over 40 channels in the 2.4 Gigahertz (GHz) range, and three of these channels are used for the advertisement of data. BLE Packets are also sent periodically instead of continuously which helps in its power efficiency. BLE can handle up to 20 connections at the same time, as compared to classic Bluetooth which can establish only up to 7 connections simultaneously mainly because it transfers small packets of data. (Riyas, 2022)

2.1.1 BLE Definitions

Generic Access Profile – It has the acronym GAP, and its responsible for controlling the connections and advertising in Bluetooth, hence handles visibility of devices and how two devices interact with each other. (adafruit.com, 2022)

Central Devices – These are devices with more processing power and memory resources that devices connect to. Examples are mobile phones and tablets. (adafruit.com, 2022)

Secondary Devices – These are devices with limited resources that connect to a more powerful central device, such as a heart rate monitor (adafruit.com, 2022)

Broadcasting Power – Also referred to as Transmit Power, it is the power with which a BLE device transmits its signal. The value ranges from -40 decibel milliwatts (dBm) to +4dBm. (estimate.com, 2022)

Advertising Interval – This is the time interval at which BLE devices broadcast their signals and it ranges from 100 milliseconds (ms) to 2000 ms. The advertising interval impacts the signal strength and power consumed by the device, with longer intervals having less stable signal but more battery life for the device and vice-versa. (estimate.com, 2022).

Received Signal Strength Indicator (RSSI) – The RSSI illustrates the strength of the signal of a broadcasting device as seen on the receiving device. It depends on the distance between the two devices and the transmit power of the broadcasting device. For broadcasting devices with maximum transmit power (+4dBm) the RSSI value usually ranges from -26 dBm to -100 dBm for distances of inches to 50 metres (m) respectively. (estimate.com, 2022)

Measured Power - The measured power is a constant which denotes the expected RSSI value read on a receiving device at a distance of 1m away from the broadcaster. This value allows one to estimate the distance between the devices when combined with RSSI. (estimate.com, 2022)

2.1.2 BLE Advertisement

Three primary channels from the 40 channels are used for advertising for BLE devices, and they are channels 37, 38 and 39. The rest of the channels are therefore secondary channels used for data transfer and transmission as pointed out by (Riyas, 2022). BLE devices send out advertisement using the Advertising Data Payload and the Scan Response Payload. The Advertising Payload is mandatory, and it is constantly transmitted by the device to let the central devices in range know that it is around. It contains up to 31 bytes of data. The Scan Response Payload is a non-compulsory payload that the central device can request for to obtain more information about the advertising device such as the device name. It can also contain up to 31 bytes of data. (adafruit.com, 2022). The advertisement process begins with the BLE device broadcasting its advertising data with its advertising interval. If a receiving device is in range and the BLE device has a scan response payload, it can optionally request for that payload to get additional data, and the BLE device responds with it. Some peripherals advertise themselves for subsequent connection and data exchange, but others just advertise data. When a connection is established between a BLE device and a central device, the advertising process stops. (adafruit.com, 2022)

2.1.3 BLE Scanning

Passive Scanning – This involves a central device scanning for advertisement data from a BLE peripheral without sending any scan request. The central device scans to receive advertisement data only (Digital Matter Support, 2020).

Active Scanning – Here, the central device scans for advertisement data and sends a scan request to the advertiser. The aim is to receive advertising data and scan response data. (Digital Matter Support, 2020)

2.2 AirTags Overview

The AirTag is a device released by Apple in April 2021 (Clover, 2022). It is a device that is used for tracking various items as long as it is attached to it such as keys and wallet. (Apple, 2020) Apple leveraged its extensive "Find My" network in its design and with the use of BLE and Ultra-Wide Band (UWB) technology, a user is able to keep track of their items on their radar wherever they are using AirTags. The AirTag is registered on a user's iPhone and is able to keep track of the device through the Find My network on their phone. When an item attached to the AirTag is misplaced, the iPhone can be used to make the AirTag play a sound for the user to trace the sound and find the item. When the AirTag is lost, and the user places it in lost mode, the AirTag sends a notification when it is detected by another user in the Find My Network. (Clover, 2022). When a lost AirTag is found, any smartphone with Near Field Communication (NFC) technology can scan the AirTag to bring up the contact information of the owner of the AirTag. In lost mode, it relays its current location back to its owner through the Find My network. Also, the AirTag is designed to alert the user when it is left behind. If an AirTag owned by someone else has been travelling with someone for a while, an alert will be sent to the supposed tracked victim's iPhone if they have one, warning about an AirTag detected when they return to a location that is frequented such as a home or office. There is also a sound played by the AirTag to announce its presence within an eight-to-twenty-four-hour period after being separated from its owner as another warning mechanism. All these discoveries were noted by (Clover, 2022)

2.2.1 AirTag reverse Engineering

A thorough study done by Adam Catley (Catley, 2022) deep-dived into discovering the technical details of the AirTag, including the security research, software, hardware details and capabilities. He focused on the low-energy design of the device that affected its battery life, the implementation of BLE and UWB technology in the device, and the privacy features offered by Apple to prevent unwanted tracking. He made some key facts and findings:

- The AirTag uses on the market components with the exception of Apple's U1 chip.
- The AirTag has a potential of 10 years of battery life because of its sleep current consumption of 2.3 micro amperes (μA).
- The device updated its BLE address and public key once a day every 04:00 am.
- The last byte of advertisement data was updated every 15 minutes.
- The device entered lost mode after 3 days of separation from the owner.
- It had an advertising interval of 2 seconds when away from its owner's device.
- The AirTag had a BLE connection interval of 1 second when near its owner's device.

He was able to identify operating states of the AirTag. They included:

Not Registered – This state refers to when the AirTag is brand new, been reset, or been removed from the Find My network. In this state it waits to be connected while having an advertising interval of 33ms.

Connected – This state is when it is connected to a registered device. No broadcasts occur in this state.

Disconnected – This state occurs when its owner's iPhone is out of range. It has an advertising interval of 2000ms.

Out of Sync – This state occurs when the AirTag reboots while separated from its owner's iPhone.

Lost – This state occurs 3 days after being in Disconnected or Out of Sync state. It then moves into Waiting for Motion state.

Waiting for Motion – This state of the AirTag is when it samples the accelerometer every 10 seconds until motion is detected.

Sound Alert – This state is when the AirTag receives a command from its connected device to play a sound or when in Waiting for Motion state and a motion is detected. It lasts for a maximum of 20 seconds.

Precision Finding - This state is triggered by the connected iPhone and is overridden by Sound Alert mode.

He discovered the AirTag has three antennas, the Bluetooth Low Energy, NFC and Ultra - Wideband.

He observed the BLE advertising packet behaviour when registered to an iPhone and the FindMy network. An illustration of the Advertising packet as described by (Catley, 2022) is shown in Table 2.1.

Table 2.1 – Advertising Data of registered AirTag by (Catley,2022)

Byte Number	Value
0	0x1E
1	0xFF
2-3	0x004C
4	0x12
5	0x19
6	0x19
7-29	Varied
30	0-3
31	Varied

After the study, some privacy concerns were raised about the AirTag. He noted that:

- The sound alerts that occur when the AirTag is away from its owner are not frequent and unlikely.
- The speaker in the AirTag could be disabled.
- The location of the AirTag can be spoofed with a replay attack.

2.2.2 The AirTag and UWB

Ultra-Wideband (UWB) radio signals are signals with high bandwidth (Mearian, 2019). A device can be classified as UWB if they have a bandwidth higher than 500 Megahertz (MHz). (Ramos, Lazaro, Girbau and Villarino, 2016) Ramos et al. noted that according to the FCC, the frequency range allotted for UWB Technology is between 3.1 GHz to 10.6 GHz, however the allowed power transmission limit is -41.3dBm/MHz. This low power also contributes immensely to the long battery life of devices like the AirTag (Amaldev, 2021). UWB systems are used for localization by utilizing time of flight of signals. Hence, a UWB tag is able to pinpoint precise location based on pings of other UWB sources near it. The U1 chip in the AirTag uses UWB technology this way for Precision Finding as suggested by (Amaldev, 2021). The U1 chip is present in the iPhone 11 and subsequent versions. As a result, these iPhones act as a UWB source and when an AirTag is pinged with it, using the Time of Flight and the angle of arrival of the signal, the AirTag is able to determine the precise location with an accuracy of a few centimetres. This location is shown in the Find My app of the owner's iPhone.

2.3 Apple Tracker Detect App

Tracker Detect is an Android app released by apple to provide a solution for users with android devices to detect if an AirTag is tracking them by scanning for them. According to (Oram, 2022) if the app detects the AirTag for 10 minutes it allows the user to play a sound to find it. It also offers the user the ability to obtain more information about the AirTag such as if it is in Lost Mode, and instructions on how to disable it. However, a major limitation is that it is a very manual process, as the app stops scanning if an AirTag is not detected after 90 seconds.

2.4 Tracking Anonymized Bluetooth Devices

(Becker, Li and Starobinski, 2019) presented an address-carryover algorithm that exploited the asynchronous nature of payload and address changes in BLE devices to achieve tracking of these devices beyond their address randomization cycles. Since BLE powered devices do their advertisement on non-encrypted public channels, they are prone to tracking and to diminish that flaw, these devices employ the use of periodically changing random addresses to make the work of trackers difficult. This research illustrated an effective way of passively monitoring these devices. They also introduced an identity-exposing attack via a device accessory that allowed permanent non-continuous tracking of BLE devices. They also presented an iOS side-channel

which enabled one to have an insight into user activity on the devices. They considered techniques in passive analysis of the signals of BLE devices where an adversary reads and observes the advertising messages but never actively modifies the traffic. The authors analysed logged BLE advertising packets in their raw format. They did this to identify potential identifying tokens which occurred in the advertising messages. Definition 2.4 explains an Identifying token as described by (Becker, Li and Starobinski, 2019). The authors proposed that Identifying Tokens may be found by analysing the raw Advertising payload and then extracting a sequence of bytes which are long enough and fulfilled the requirements as explained in Definition 2.4, or by breaking down the payload according to Bluetooth specification and identifying suitable metadata elements. The idea for a suitable length for the Identifying Token is to ensure uniqueness and prevent collision as much as possible. They noted that finding an Identifying Token for a class of device can be used to track any individual device in this class of devices.

Definition 2.4 – An Identifying token is any sequence of bits in an advertising packet that can be used to distinguish one device from another whether by design or by side effect.

2.5 Detecting BLE Devices in High Density Scenarios

Here, the authors (Hernandez-Solana et al., 2018) analysed backoff in Neighbour discovery process (NDP) of BLE which is based on active scanning. Since NDP is essential for Internet of Things (IoT) devices with regards to detecting a large and varying number of devices in a short time, they proposed a simple and practical adaptation of backoff in NDP on scanner functionality. They presented a new backoff scheme and together with the proposed adaption they were able to improve the discovery latencies of BLE devices, and thus led to high probability of discovering a large number of devices in high density situations.

2.6 Tracking and Monitoring items with Arduino Based Device

(Adjei et al., 2020) presented the design of an Arduino based device which tracked and monitored any valuable items that a user wanted monitored within a range of 10 meters at all times in real-time. The authors introduced a physical design and a simulated counterpart to compare the reliability, cost and speed. They used Bluetooth connection to interface between the user's phone and the Arduino device. The results of their project demonstrated that as soon as connection is lost, a call was made from the tracked device to the user's phone to signal a disconnection, while an alert message containing the current location of the disconnected device was sent via Global

System for Mobile Communications (GSM). They were also able to demonstrate that after every 1000 milliseconds, updated coordinates were sent to the user, for tracking the device even with constant location changing.

2.7 Visualization of Vehicle Movements on Android Phone using Bluetooth

(Ahmed et al., 2016) presented an Android application that enabled the visualization of the movements of vehicles in real-time on Google Maps using Dedicated Short-Range Communication (DSRC) and Bluetooth communication. The android application received key information such as the position, speed and direction of mobility of vehicles through the GPS receiver attached to their DSRC unit. The application also communicated with one of the DSRC units using Bluetooth to obtain real-time traces collected from all vehicles equipped with the DSRC unit. As a result, the authors were able to use the android application to display live movement of these vehicles on Google Maps together with their path history, speed and direction.

2.8 Tracking Movements of Football Players Using Wearable Devices

(Kim et al., 2019) presented a prototype wearable device that tracked movements of football players during the match time. The wearable device with the help of several realized algorithms on the embedded processor was able to estimate the amount of speed, distance covered and inertia that the football players possessed. This crucial data was transferred from the device using Bluetooth Low Energy (BLE) protocol. They agreed that the use of BLE reduced the overall power consumption of the device. Their experimental results demonstrated that the BLE-based wearable device successfully illustrated the real-time tracking operation, achieving a low-power solution in comparison to existing devices.

2.9 A child tracking system to monitor children using Alarm Technique

(Isa et al., 2019) noted the recent rise in cases of missing children especially in open and crowded venues and hence proposed a child tracking system to help parents monitor their kids. They presented a device which raised an alarm when the Bluetooth connection is disconnected between the parent and the child. An implemented GPS application used on the phone of the parent was used to track the location of the missing child wearing this device. The proposed system was therefore made up of two main units, one for parents and the other for child. The child's unit acted

as a broadcasting device which transmitted a GPS signal, while the parent's unit received the signal to determine the position and distance of the child.

2.10 Privacy Concerns

2.10.1 Risk of Location Compromise with Mac Addresses

(Kikuchi and Yokomizo, 2013) presented the experimental results on scanning Mac address of Bluetooth devices and showed the risk of location privacy to be compromised from the Bluetooth scanning. From their study, more than 70 percent of users carried devices with Bluetooth capabilities, with a quarter of those users having their Bluetooth status always active which made them prone to scanning. In their experimentation, 1.26 people out of a population of 100 had been detected in a day, revealing their MAC addresses. The Bluetooth detection server developed by the authors was capable of gathering vital information and behaviours about the MAC addresses of the Bluetooth devices. It collected information such as how often the devices access a particular location and the time the devices left the location. This study established that there is a risk of location privacy being compromised by Bluetooth scanning.

2.10.2 Security Vulnerabilities of BLE Protocol

(Barua et al., 2022) analysed the BLE protocol and identified security flaws that could lead to security and privacy issues. They presented a comprehensive taxonomy for the security and privacy issues of BLE by presenting possible attack scenarios for different types of vulnerabilities, classifying them according to their severity, and listing possible mitigation techniques. They introduced a threat model for all the possible attack scenarios. However, the authors also offered recommendations for alleviating these threats through the help of tools. They finally discussed new features and potential for novel application domains that will be the driving force for the usage of BLE in future IoT devices.

2.11 Metrics for Evaluation

2.11.1 Accuracy

We are designing a system to detect the presence of AirTags. The tests to be performed will primarily involve predictions of whether the AirTag is detected or not and the accuracy of detection will be used to evaluate the overall performance of the system.

2.11.2 Precision

The rate at which positive detections of the AirTag are accurate will be calculated to also measure the performance of the system.

2.11.3 Sensitivity (True Positive Rate)

In measuring accuracy of data samples, the overall accuracy may not be enough to assess the overall performance of the system, hence the actual positive detection sample will be covered and assessed. It is also the true positive rate.

2.11.4 False Positive Rate

To determine the rate at which false results are detected by the system, the False Positive Rate will also define how successful the implementation of the system is.

2.12 Summary

In this chapter, we discussed Bluetooth and BLE Technology extensively, and how devices advertise data and packets which make them prone to attacks, mainly passive scan attacks.

We consider the AirTag and discuss how it operates and the known properties so far. Knowing this context benefits the research. Also, Apple's own Android app is looked at closely to examine what can be improved.

We also discuss research that have used BLE technology to track various people, and items using a plethora of techniques. The privacy concerns raised by Bluetooth/BLE tracking and usage was presented too.

With all the information discussed, we look to extract information from BLE Packet of the AirTag to determine an Identifying Token, and thus to provide a reliable mechanism for detecting AirTags.

Chapter 3

Methods

3.1 Environment Setup

3.1.1 Laptop

The software framework and environment used for the project was executed on a Dell Inspiron 7577 laptop with the following specification:

- Operating System – Windows 10
- CPU - Intel Core i7-7700 HQ, 2.8 GHz
- Memory – 16 GB RAM + 1000 GB HDD

3.1.2 Android Smartphone

The implementation of the android application was run and tested on an Alcatel 1 5033XR with the specification below. The experiments were also conducted using the application on the android phone.

- Operating System – Android 11
- CPU – MT6739
- Memory – 1 GB RAM + 16 GB Phone Memory
- API Level – 31

3.1.3 AirTag

One AirTag was used in the research, implementation and testing process. Another AirTag was used for validation and used together with the first one during experimentation. Their serial numbers are shown below:

- HGGHFH6TP0GV
- HGRJ5FPWP0GV

3.1.4 Apple iPhone

An Apple iPhone was the registered iPhone for the AirTags. It was used during the research and testing phase in tandem with the AirTags. The specification is shown below:

- Model – XS Max
- Operating System – iOS 15
- CPU – Apple A12 Bionic
- Memory – 4GB RAM + 512GB Phone Memory

3.1.5 Software Development Environment

The programming language used for implementation of the android application was Kotlin. Kotlin is used because it allows Android apps to be developed faster and is used by over 60 percent of professional android developers (Android Developers, 2022), hence a lot of support was readily available.

The open-source integrated development environment (IDE) used was Google's official Android Studio. This allowed the easy use of the official BLE Application Programming Interface (API) provided by Google (Android Bluetooth le | Android Developers, 2022). The open source BLE API was used to implement the critical BLE parts of the android application.

The Jupyter Notebook IDE was the environment used to build the Linear Regression Model as well as the plots and functions for validation testing using Python 3 programming language.

The WEKA tool was used to run machine language algorithms on the created dataset to evaluate accuracy metrics.

3.2 Detecting BLE Devices

3.2.1 Simple BLE Scanning Implementation

One of the main ideas of the project was to be able to detect an AirTag which is a BLE device. To do that, BLE devices needed to be detected first. Using the BLE API, a simple android application was implemented to scan for nearby BLE devices and display information such as Device Name, MAC Address, RSSI value of each individual device in the scan result. The following Bluetooth LE Permissions were declared in the implementation:

- Bluetooth Permission
- Bluetooth Admin Permission

The Bluetooth Adapter was initialized and implemented since it is required for any Bluetooth activity.

For Scanning, the *BluetoothLeScanner* class (BluetoothLeScanner | Android Developers, 2022) was used and implemented to find discoverable devices in the vicinity.

The *ScanSettings* mode implemented was SCAN_MODE_LOW_POWER (ScanSettings | Android Developers, 2022). This mode consumes the least power and was used to enable long period of scanning.

The *ScanRecord* functionality as described by the API (ScanRecord | Android Developers, 2022) was used to fetch the earlier mentioned information of the devices from their advertising packets.

The *ScanResults* (ScanResults | Android Developers, 2022) functionality was used to display the information of the devices.

Discoverable BLE devices in range were detected by the application.

3.3 Analysing and Extracting Advertisement Packets

3.3.1 Parsing Device Advertisement Data

The *getBytes* method of the *ScanRecord* class was used to obtain the full advertising data packet of the scanned devices. Since it was in *ByteArray* format, the initial format was parsed to convert it into a meaningful string hexadecimal format.

3.3.2 Analysing Advertisement Features

The scan results now displayed devices with their readable full advertising packet. Most of the devices had no name in the scan results, as a result, the various advertising packets were analysed. Table 3.1 shows devices captured and their respective advertising packets

Table 3.1-Some BLE Devices and the Advertising Packets

Name	MAC Address	Advertising Packets
Unnamed	61:95:6C:2F:EE:89	0x02011A020A0C0AFF4C0010051618181A07
Unnamed	DB:2F:86:BF:09:8C	0x1EFF4C00121910F0B9551C79E23EED5298A6EC89AC9ECC 0AD933856CAC0059
Unnamed	23:EC:B7:25:75:D2	0x19FF060001092102D9A1FB8B25D44A4546464552534F4E2 D5043

Unnamed	CE:65:14:2D:80:00	121910510A7F589875B8804A90CAA6920F534A43D861FF902E02A8
Unnamed	EF:D8:27:34:6E:3E	0x07FF4C0012020003

3.4 Identifying and Extracting AirTag Advertising Data

3.4.1 AirTag Identity

The various advertising packets were analysed thoroughly to be able to identify which of the results were the AirTags. The advertising packets were compared with the byte data in the research done by (Catley, 2022) to identify the AirTag. The RSSI value with respect to the distance between the AirTag and the receiving phone was observed carefully. High dBm values showed the distance was close, while lower dBm values showed the distance was relatively larger. The AirTags were identified to be device number 2 and 4 as shown in Table 3.1.

3.4.2 Extracting AirTag Advertisement Data Features

The identified AirTags were further analysed over time to obtain more information about them. According to Android's BLE API, scan results can be filtered using *scanfilters* (ScanFilter | Android Developers, 2022) using the following parameters:

- Name of Bluetooth LE device
- MAC Address of BLE device
- Manufacturer Specific Data of the device
- Service UUID of the device
- Advertising data type and corresponding data

Conforming to the research of (Catley, 2022) and as noted by (Silicon Labs, 2022), the Advertising Data Type of the AirTag is the Manufacturer Specific Data. The Manufacturer Specific Data (MSD) is defined in Definition 3.4.2 below. The *getName*, *getAddress*, *getManufacturerData* methods as defined by the *ScanRecord* class were used to obtain information about the Name, MAC Address and MSD respectively, to analyse and extract features. The *getTxPowerLevel* method was used to derive the Measured Power (MP) of the AirTags too. Table 3.2 shows sample features that were extracted. Since the device name is not advertised, we set the scan results display

device name as “Unnamed”. The measured power value was also not set, indicating that it was not part of the advertising packet

Table 3.2 – Information Obtained from AirTag Advertising Data

MAC Address	MSD	MP
DA:6A:C1:7F:64:88	121910EC9D38DC25C76728E9893488C211CF1B18B94D3E26490310	0
CE:65:14:2D:80:00	121910510A7F589875B8804A90CAA6920F534A43D861FF902E02A8	0
DE:FE:1D:A2:53:D6	121910EB886BB7B188D786E759FD15177138D7AE650431952303E4	0
DE:FE:1D:A2:53:D6	121910EB886BB7B188D786E759FD15177138D7AE650431952303C6	0
F2:11:1B:F7:EE:BC	1219109D9C467DFC052152756B1F863437FD4EFF9163297D2103A2	0

Definition 3.4.2: Manufacturer Specific Data – It is the data associated with a particular manufacturer and it is used by the manufacturer to add any custom data into the packet (Silicon Labs, 2022).

3.5 AirTag Identifying Token

From careful observation of extracted features of the advertisement pack, it was noted that the first 3 bytes of the MSD were always constant no matter the changes to the MSD. These first three bytes and the remaining structure also coincided with the research by (Catley, 2022) on the structure of the advertising packet of AirTag when registered. Since this sequence of bytes were always constant and were able to distinguish themselves from other devices as suggested by (Becker, Li and Starobinski, 2019), they were determined to be the Identifying Token of the AirTag. The Identifying Token was therefore **(0x12, 0x19, 0x10)** or **(0x121910).**

3.6 Scan Filter

3.6.1 Parsing Identifying Token

Before using the identifying token as a filter, it was converted into the form *ByteArray* as specified by the BLE API. The hexadecimal string of 0x121910 was parsed into type of *ByteArray* to be used by the filter.

3.6.2 Filter Construction

The identifying token is a byte sequence in the manufacturer specific data. The scan filter was constructed using the *ScanFilter Builder* class with *setManufacturerData* filter option using the following tokens as specified by the BLE API (ScanFilter.Builder | Android Developers, 2022):

- Manufacturer ID – 0x004C (which represents Apple's company identifier)
- Byte Array – 0x121910

3.7 Measured Power

3.7.1 Signal Strength at Varying Distances

The measured power (MP), also known as the one-meter RSSI (Shah, 2022), of the AirTag has not been set and is not known, and as a result was estimated through experimentation. The average signal strength of the AirTag was recorded over multiple distances of 0.02m, 0.10m, 0.25m, 0.5m, 0.75m, 1m, 1.5m, 2m, 2.5m, 3m, 5m, 7m and 10m and at different angles of 0 degrees, 90 degrees, 180 degrees and 270 degrees as shown in Appendix B2. The mean of these values were calculated as shown in Table 3.3. These RSSI values at the respective distances were used to build a linear regression model.

Table 3.3 – Average RSSI values over Distance by AirTag

Distance (m)	RSSI (dBm)
0.02	-26.25
0.10	-39.75
0.25	-46.00
0.50	-50.00
0.75	-53.00
1.00	-58.50
1.50	-63.50
2.00	-65.25
2.50	-72.00
3.00	-72.25
5.00	-80.25
7.00	-81.75
10.00	-83.75

3.7.2 Linear Regression Model

A linear regression model was implemented to determine the RSSI value at 1m, i.e., the measured power. Using the Linear Regression libraries from Python such as *Numpy, sckit-learn* and *statsmodels*, a model was created using the data. The implementation is shown in Appendix C1. The parameters for the intercept and slope were found as:

- Intercept: -48.67482470990923
- Slope - -4.74352406

To determine the validity of the model, three tests were performed:

- The line of best fit was plotted over the distribution to observe if it fits the data. This implementation is illustrated in Appendix C1.
- A residual plot was plotted to observe how randomly the residuals are scattered over the distance to check for heteroscedasticity (Appendix C1). Heteroscedasticity is defined in Definition 3.7.2 below by (Statology, 2022).
- The Coefficient of Determination (R^2) was evaluated to tell which amount of variation is RSSI value can be explained by the dependence on the distance value using the linear regression model constructed. The calculation implemented with python is shown in Appendix C1.

The model was then used to predict the signal strength at 1m, which represents the measured power. The model predicted a measured power of -53.418 dBm.

Definition 3.7.2 – "In regression analysis, heteroscedasticity refers to the unequal scatter of residuals or error terms".

3.8 Distance Estimation

The estimated distance based on the current RSSI value can be calculated using the formula shown in Definition 3.8. as indicated by (Shah, 2022). The parameters involved include:

- The distance (to be estimated)
- Measured Power
- RSSI value
- N, a constant which represents low to high strength of the signal based on environmental factors

For this project, N = 4.5 was utilized, because the AirTag has a relatively high transmit power of about 4.5 dBm (fccid.io, 2020). Using the earlier determined measured power value, the estimated distance was able to be measured based on the current RSSI value measured by the android phone. This formula and parameters were implemented in the android application as follows, with estimated distance displayed in the scan result:

Implemented Formula – Distance = 10 ^ ((-53.4 – (current RSSI)) / (10 * 4.5))

Definition 3.8 – Distance = 10 ^ ((MP – (current RSSI)) / (10 * N))

3.9 Alert System

A notification alert system was implemented using Androids Notification API (Notifications | Android Developers, 2022). A time period of one (1) minute before an alert was given, was used to simulate a period after detection of an AirTag. The notification priority type implemented was set at High Priority to make the alert process very evident.

3.10 Creation of Dataset

Experiments were carried out to test the success of the android application which was using the implemented filter made with the Identifying Token. The experiments were to primarily determine:

- If an AirTag is correctly detected – Experiment A
- If an AirTag is correctly not detected – Experiment B

Each experiment lasted three (3) minutes and the outcome was recorded. To prevent imbalanced classification, oversampling technique was used with Experiment B to prevent a severe skew in the class distribution of the data (Pykes, 2020). The classes were

- Detected
- Not Detected

A total of 100 data points were recorded for Experiment A. As a result, 100 experiments were carried out and recorded for Experiment B. Both AirTags were used for the experiments. A data point refers to any data from the scan result on the Android Application collected from experiments with either or both of the AirTags. The variables of the dataset include:

- Experiment Number

- Flag
- MAC Address
- Advertising Data
- Manufacturer Specific Data
- RSSI at 0.02m
- RSSI at 0.5m
- RSSI at 1m
- RSSI at 3m
- RSSI at 5m
- Distance Measured at 0.02m
- Distance Measured at 0.5m
- Distance Measured at 1m
- Distance Measured at 3m
- Distance Measured at 5m
- Detected

The Experiment Number Attributes denotes the data record number. The Flag attribute denotes the state of the Bluetooth availability of the owner's iPhone. 0 means the Bluetooth of the iPhone is off while in range, while 1 means the Bluetooth of the iPhone is on while in range. The Advertising Data denotes the full advertising packet recorded. The MSD denotes the MSD recorded. The RSSI at varying distances denotes the signal recorded at those specified distances. The Distance Measured at varying distances denotes the estimated distance recorded at those specified distances. The entire raw dataset is shown in Appendix B.1.

3.11 Testing

3.11.1 True Positives

The experiments carried out in Experiment A tested for true positives. A true positive occurred when the AirTag was in range and it was detected, with the registered iPhone with Bluetooth status: OFF

3.11.2 True Negatives

The experiments carried out in Experiment B tested for true negatives. A true negative occurred in two instances:

- when an AirTag was not detected when it was not in range
- when an AirTag was in range, but with the accompanying registered iPhone with Bluetooth status: ON

3.11.3 False Positives

A false positive occurred during experimentation if any of these situations were recorded:

- Another BLE Device apart from an AirTag was detected in the scan result
- Detecting an AirTag when accompanying registered iPhone was in range with Bluetooth status: ON

3.11.4 False Negatives

A false negative occurred during experimentation if any of these situations happened:

- The AirTag is not detected while in range and with accompanying registered iPhone with Bluetooth status: OFF
- The AirTag is not detected while accompanying registered iPhone is out of range.

3.11.5 Signal Strength at Varying Distances

The signal strength at varied distances of 0.02m, 0.5m, 1m, 3m and 5m (if possible) by the android application were determined and recorded with every experiment.

3.11.6 Estimated Distance at Varying Distances

The distance estimated by the application at distances of 0.02m, 0.5m, 1m, 3m and 5m (if possible) were also determined and recorded with each experiment.

3.12 Summary

To conclude this chapter, we describe the implementation of the android application system which detects AirTags and capable of alerting.

The techniques shown in the sections carefully demonstrate how a simple BLE scanner was built, and used to detect BLE devices, analyse their advertising packets and extract required information from it. The research presented in Subsection 2.2, in addition to careful observation, aided in identifying which device from the results was the AirTag. An identifying token for the AirTag was extracted and used to build a scan filter which detects AirTags. The identifying token as described by (Becker, Li and Starobinsky, 2019) that was used for our implementation was the byte sequence: 0x121910. It is the first three bytes of the MSD of the AirTag. The implementation of the filter to the simple scan application morphed it into an AirTag detecting application.

The measured power of the AirTag was determined using a Linear Regression Model to be able to estimate distance of the AirTag away from the Android Phone. The formula used for the implementation was: Distance = 10 ^ ((-53.4 – (current RSSI))/(10 * 4)). The estimated distance feature is to help locate a detected AirTag.

Experiments were conducted to determine the accuracy of the system in correctly detecting and not detecting an AirTag. The results were recorded in a dataset.

Chapter 4

Results

In this chapter, we present the results obtained from the methods implemented in chapter 3. The resultant android application and its functionality is looked at. The results of validity test for the Linear Regression model is also touched on. The results of the experiments as recorded in the dataset is described in this chapter. The accuracy metrics which describe the effectiveness of the implemented system are also explained.

4.1 Android Software Application

A functioning android application was implemented capable of scanning for nearby AirTags, detecting them, displaying some advertising packet details, and alerting the user after detecting an AirTag. The details showed in the scan result are listed below:

- MAC Address
- RSSI value
- Manufacturer Specific Data
- Estimated Distance

Figure 4.1 illustrates the view of the application before scanning is executed.

Figure 4.2 illustrates the view of the application after detecting a supposed AirTag.

Figure 4.3 illustrates the view when an alert is made after detecting a supposed AirTag after a time period (1 minute).

Because the design and implementation decision was to use scan setting SCAN_MODE_LOW_POWER without any scanning period restrictions, scanning could be done continuously for as long as 24 hours without manually stopping it. This relatively long scanning period allowed for maximum window for detecting supposed AirTags and alerting. This was unlike Apple's Tracker Detect App described in Section 2.3 that allowed a maximum scanning period of 90 seconds.

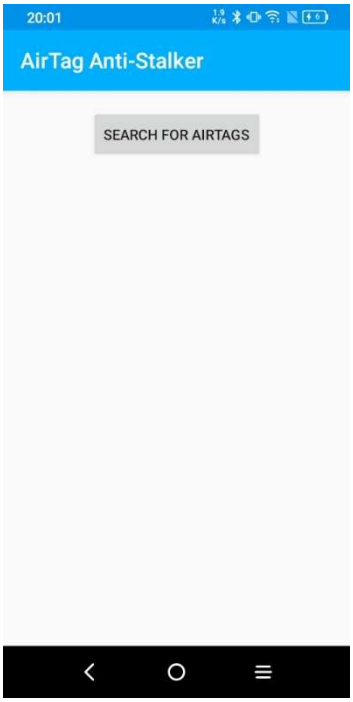

Figure 4.1 – Home View of Application

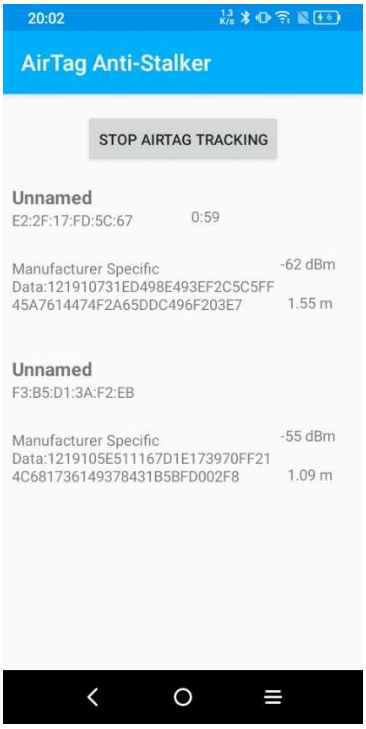

Figure 4.2 – Detection View of Application

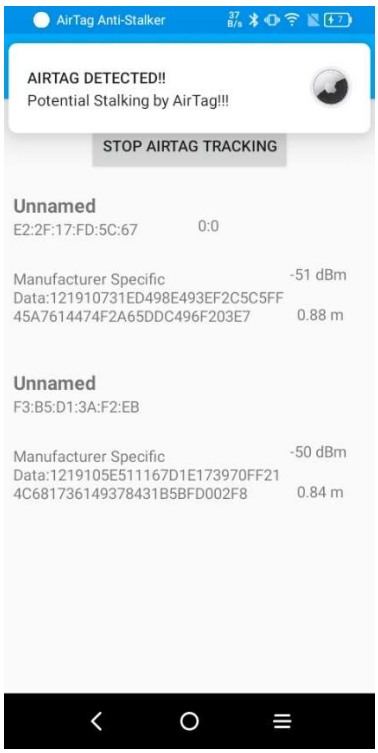

Figure 4.3 – Alert Notification View of Application

4.2 Validity of Linear Regression Model

4.2.1 Line of Best Fit

To assess whether the Linear Regression model constructed fits the data, a line of best fit was plotted. This is shown in Figure 4.4. From observation, the model somewhat fits the data.

4.2.2 Residual Plot

Another validation analysis was performed by plotting a residual plot to check for the heteroscedasticity of the residuals. This is shown in Figure 4.5. From observation, the residuals are somewhat randomly scattered around zero, hence indicating that heteroscedasticity is not a problem with the independent variable, distance, and that the data fits the model.

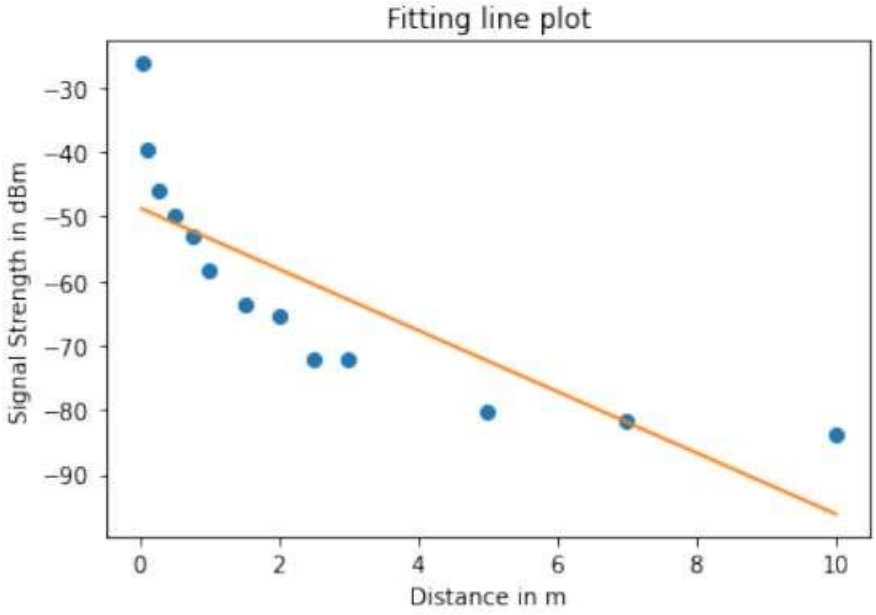

Figure 4.4 – Fitting Line Plot

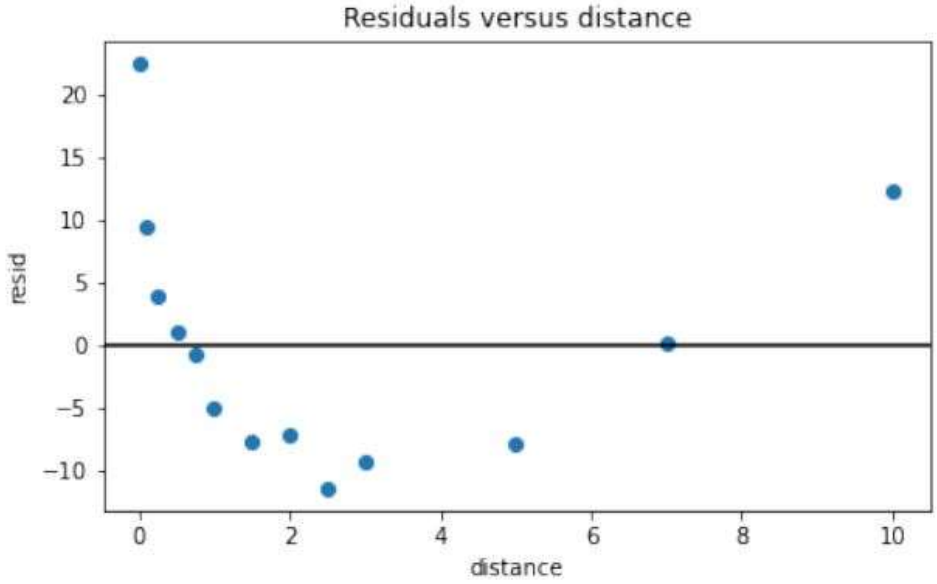

Figure 4.5 – Residual Plot

4.2.3 Co-efficient of Determination (R^2)

The co-efficient of Determination tells which amount of variation in "RSSI" can be explained by the dependence on "distance" using the linear regression model built. The value is between 0 – 1. The R^2 value calculated for this model was 0.6778668358892557. Larger R^2 value indicates a

better fit and means the model can better explain the variation of the output with different inputs. The R^2 value shows that the Linear Regression Model is an optimum fit.

4.2.4 Conclusion

The results of the validation tests validated the use of the Linear Regression Model with the following parameters as a good model to predict the estimated Measured Power of the AirTag:

- Intercept: -48.67482470990923
- Slope - -4.74352406

4.3 Experiment Results

4.3.1 AirTag Detection

From the experiments, the Android Application was capable of detecting AirTags using the filter created with the identifying token. In scenarios where an AirTag was to be detected, that is, if an AirTag was in range and was broadcasting its advertising packet, the Application was capable of detecting it. In the scenarios where an AirTag should not be detected, the system correctly did not detect it. These scenarios included if the AirTag was out of range, or the AirTag was not broadcasting its advertising packet. No other BLE device was detected using the android application with the implemented filter even when they were in range and broadcasting advertising packets apart from the AirTags. The ability of the android application to correctly detect only the AirTag demonstrates that the Identifying Token determined for the AirTag is right and appropriate. The raw results for detection and non-detection of the AirTag are shown in Appendix B1.

4.3.2 Estimated Distance

From the experiments, the estimated distances of the AirTags away from the phone were able to be calculated. Because RSSI fluctuates as a result of many factors such as angle between two devices, environmental factors, absorption presence of obstacles, diffraction (estimate.com, 2022), the estimated distances determined were not constant for a particular actual distance. Moreover, the estimated distances were more often than not unequal to the actual distances. However, these estimated distances were able to give a good idea of how close or far the phone was to the AirTag. In addition to the RSSI value, the AirTag could be located with the estimated distance value. The raw results for estimated distances determined over actual distances are also shown in Appendix B1.

4.3.3 Conclusion

We demonstrated that AirTags can be identified and detected with the identifying token (0x121910 of the MSD). Also, other BLE devices were not detected using the filter made with the Identifying token. This showed that the identifying token is unique enough for the AirTag.

Also, we established that though estimated distances were not equal to the actual distances, they were capable of giving a suitable idea of how far or close the receiver, the phone, was to the broadcaster, the AirTag.

4.4 Accuracy Metrics

The metrics for accuracy of the system were determined by using machine learning algorithms. The algorithms used were Naïve Bayes, Support Vector Machine and Random Forest. The full results for each of the algorithms is shown in Appendix B3.

4.4.1 Accuracy

The accuracy of the system indicates the rate of correct predictions made by the system (Gad, 2020). In this case, it tells how accurate the system correctly detects an AirTag and does not. Table 4.1 shows the accuracy of the system.

Table 4.1 – Accuracy of System

Algorithm	Naïve Bayes	Support Vector Machine	Random Forest
Value	98.5	99.5	99.5

4.4.2 Precision

The precision value details how accurate the positive predictions are (Gad, 2020). Here, it denotes how accurate the system is at detecting AirTags correctly. Table 4.2 illustrates the precision of the system:

Table 4.2 – Precision of System

Algorithm	Naïve Bayes	Support Vector Machine	Random Forest
Value	0.985	0.995	0.995

4.4.3 Sensitivity

The sensitivity, also known as the true positive rate, explains how accurate positive detections were made based on experiments to find positive detection results (Gad, 2020). Table 4.3 shows the sensitivity of the system:

Table 4.3 – Sensitivity of System

Algorithm	Naïve Bayes	Support Vector Machine	Random Forest
Value	0.985	0.995	0.995

4.4.4 False Positive rate

The rate at which incorrect detections were made by the system (Gad, 2020), which is False Positive Rate, was determined. Table 4.4 shows the False Positive Rate of the system as evaluated by the algorithms:

Table 4.4 – False Positive Rate of System

Algorithm	Naïve Bayes	Support Vector Machine	Random Forest
Value	0.014	0.005	0.005

4.4.5 Conclusion

We present the various accuracy metrics to evaluate the validity of the system. The system has an average accuracy of 99.17%, precision of 0.992, sensitivity of 0.992, and false positive rate of 0.008. The full results evaluated by the machine learning models are shown in Appendix B3.

4.5 Security Analysis

4.5.1 Positives

The AirTag broadcasts its advertising packet only when it is not connected to its registered iPhone. The system displayed a detected AirTag distinctly as long as it was in range. The last byte of Manufacturer Specific Data of the AirTag changes randomly every 15 minutes exactly on the hour, the quarter past, the half hour, and the quarter to each hour. This occurs while advertising without any disturbances. Here, a disturbance denotes the AirTag re-connecting to its registered iPhone and disconnecting again to re-commence broadcasting again. The MAC Address of the detected

AirTag remains unchanged throughout while AirTag is detected and undisturbed. Despite the changes to the last MSD, the system identified the AirTag as the same one since the MAC Address remains unchanged in that period.

However, with disturbances, the following changes shown in Table 4.5 occur when these scenarios described happen.

Table 4.5 – BLE Connection Disturbance of AirTag

Number	Disturbance	Effect
1	AirTag connects and disconnects within the 15 minutes interval	The MAC address and the MSD remain unchanged
2	AirTag is in connected mode while the 15-minute mark passes, and then disconnects afterwards	The MAC address changes and the last 27 bytes of the MSD change too

When the MAC Address of the AirTag changes it is seen as a new device. However, the scenario presented in Table 4.5 is the only way the MAC Address changes in a 24-hour period. This implies that as long as an AirTag is nearby and is broadcasting without interruptions, the system is able to detect it even when the MSD keeps changing every 15 minutes.

4.5.2 Limitations

In the case where disturbances occur in Scenario 2 illustrated in Table 4.5, the system detects the AirTag as a new one because of the change in MAC Address.

Another limitation to consider is that when the AirTag is in connected mode, it cannot be detected by BLE scanning since it does not broadcast advertising packet in that mode. This scenario likely suggests that the owner of an AirTag is nearby and connected to the AirTag by Bluetooth. In such a scenario, since it is not possible to detect the AirTag, it becomes unclear whether the owner of the AirTag is possibly using it to stalk. Though, in most stalking situations using the AirTag

(Matei, 2022), the stalker is usually not near victim and the AirTag that is used for the stalking. Because of UWB technology as referred to in subsection 2.2.2, the stalker can be far away and out of range of the AirTag and still track it on the Find My app. This is the method most used by stalkers since it limits the possibility of being caught. As a result, we suggest that an AirTag being detected over a period of time, could potentially be used for stalking. However, in situations where a carefully hidden AirTag in connected mode is used for stalking, there is a high chance of not detecting the AirTag.

4.6 Summary

The results we present in this chapter demonstrate the implemented Android Application, and this system's capability of Detecting AirTags. We present how effective the Identifying Token is in the use of detecting AirTags uniquely. We also illustrate the validation of the Linear Regression Model using a line of best fit, a residual plot and co-efficient of determination value.

We present the results of experiments done to determine the accuracy, precision, sensitivity and False Positive Rate of the system which gives motivation for the evaluation of the system.

The analysis of the security implications of the behaviour of the AirTag and the implemented system is touched on in this chapter too.

Chapter 5

Discussion

The objectives of this study, in broad terms, are to demonstrate a mechanism that can address the issue of anti-stalking by AirTags by being able to uniquely detect them. We evaluate the various achievements made in this research based on the objectives we set and also compare them with related work. The confidence and limitations in undertaking this project are also discussed.

5.1 Results Compared to Objectives

5.1.1 Objective 1

Objective 1 – To derive an exclusive Identifying Token of AirTags to be able to uniquely identify the device.

This objective was met as we derived an Identifying Token which is able to exclusively identify AirTags. The Identifying Token determined is the first three (3) bytes of the Manufacturer Specific Data of the AirTag in its BLE Advertising packet which are 0x12, 0x19 and 0x10. These first three bytes are always constant in that position and in that sequence in the MSD. Their length and constancy in the advertising packet of the AirTag make it very suitable as an Identifying Token as (Becker, Li and Starobinsky, 2019) denoted. The careful analysis and observation of the advertising packet together with reference to extensive study done by (Adam, 2022) enabled the extraction of the Identifying Token and the completion of this objective.

5.1.2 Objective 2

Objective 2 – To design and implement an Android Application using Identifying Token to detect AirTags and alert timely.

This objective was met as a simple android application capable of identifying AirTags and alerting was implemented. Using the derived identifying token, a scan filter was implemented into the application to detect AirTags even amongst other BLE devices. The application system was capable of detecting a broadcasting AirTag as long as it was in range.

An alert notification system which prompted the user after detecting an AirTag with high priority was implemented. These mechanisms of detection and alert by the implemented android

application to challenge the problem of possible stalking with an AirTag made this objective a success.

5.1.3 Objective 3

Objective 3 – To test and analyse if the system accurately detects AirTags from other BLE devices.

This objective was met as the system was tested for its accuracy, precision, specificity and False Positive Rate with very positive results. The system had an overall average accuracy of 99.17%. The average precision of the system was evaluated at 0.992. The average specificity of the implemented system was determined as 0.992. The false positive rate was found to be 0.008. The tests showed no instance of detecting another device apart from the AirTag. These analysed results from the tests undertaken show that the implemented system accurately detects AirTags from other BLE devices and hence the achievement of this objective.

5.2 Results Compared to Related Work

Though functionality of the implemented application in this project work is similar to an extent to Apple's Tracker Detect app described in subsection 2.4 in terms of being able to detect AirTags, this project achieved more.

The project was able to achieve an estimated measured power for the AirTag. Though this value has not been provided by Apple, using a Linear Regression Model we were able to determine a placeholder measured power value of -53.418 dBm for the AirTag.

This one-meter RSSI value enabled the android application to be able to estimate the distance of the phone away from the AirTag. Together with the RSSI value, the estimated distance could help locate the AirTag. This functionality differentiates it from the Apple Tracker Detect App and adds another dimension to the anti-stalking process.

Furthermore, the ability of the application to scan continuously for AirTags for a very long period of time without stopping is another result of the work that challenges the Tracker Detect application. As mentioned, it scans for AirTags only for a period of 90 seconds. This makes the process of detection very manual. However, the ability of the implemented android application to scan for long periods makes the anti-stalking process relatively automatic.

5.3 Confidence and Limitations

Due to the time imposed for this project some limitations had to be considered:

- The optimum time before an alert is raised by the android application after detecting an AirTag to signify that stalking is most likely occurring was not studied and experimented extensively. As a result, a placeholder time of one minute before a notification alert was prompted was used.
- The other BLE devices that were used for testing were few and included the iPhone, the Dell Windows Laptop, and Apple AirPods pro. The system was not tested with an extensive list of BLE devices.
- Experiments and Model construction for determining the Measured Power of the AirTag was not thoroughly done as we would have liked due to time constraints to effectively get a more reliable measured power value. Owing to this, the calculations for the estimated distances may not be reliable enough.

5.4 Summary

We have evaluated the results of the project work in comparison to each of the objectives set at the beginning of the project. The results proved to be generally successful and completed. Also, we looked at the results of the work as compared to similar work, mainly the Apple Tracker Detect app. We finally discussed the confidence and limitations encountered during the design and implementation of this project work.

Chapter 6

Evaluations, Reflections and Conclusions

To conclude this study, this Chapter evaluates the overall accomplishments of the study carried out and reflects on the skills gained and problems encountered. The overall contribution to the field of BLE devices, tracking and anti-stalking is assessed. We also recommend future work which can build on the outcome of this project work.

6.1 Evaluation

The aim of this project was to design and implement a system used for anti-stalking with AirTags. Because of the scope of the project and the limited time available for the project, the BLE advertising process and the BLE scanning process were the areas most studied and focused on. The objectives set for the project were generally achieved as presented in the Discussion chapter.

Literature was studied to describe the context of the project and explore existing techniques in Bluetooth and BLE tracking that could be applied to the project. Also, present work and research done on the AirTag was investigated to learn about it and find more information about it. Since the AirTag is a relatively new device which was released in 2021, work documented about it was mostly online. The relatively few works which investigated the AirTag thoroughly and provided vital information about it were provided in the report.

The study of BLE related material was relatively easy due to the presence of many information available on this subject matter. A short online course on BLE helped me immensely understand the concepts and how the technology worked. This made further researching easier as I understood most of the terminologies and applications easier.

The implementation of the Android Application was not really problematic as I am familiar with object – oriented programming. However, I am not so familiar with Kotlin good practices so the application build encountered many errors at first and required a lot of modification and debugging throughout the project to achieve what was needed. Though the Android BLE API provided a lot of support into implementation of a simple BLE android application, I found myself still having to learn more to be able to achieve what was needed.

The main difficulty faced was when it came to deploying a test build of Android application after implementing the BLE features. Android Studio emulator does not support running apps running Bluetooth as at the time of implementation, hence the app could not be tested early. Much time was used to find another solution for running the test build of the app by assessing Bluestacks android emulator, and a virtual machine but to no avail. Though the plan was to eventually probably test the application on a real android phone, the purchase of the phone had to be brought forward. This debacle wasted a little precious time and was an inconvenience financially at that time.

In extracting the identifying tokens, there was a hurdle that involved parsing the advertising packet of the BLE devices into readable format before being able to analyse them. Once they were in readable format, it was relatively easier for analysis and in eventually obtaining the identifying token.

Moreover, the variation of scenarios for experimentation for more specific results in those scenarios was limited by time. This mainly applied to specific stalking scenarios and their analysis, and experimentation of signal strength in various scenarios.

The project was successful in the sense that an identifying token was derived which was able to be used to effectively distinguish an AirTag and applied in an Android Application to do exactly that. This implemented application was shown to detect AirTags with a high accuracy hence is a reliable mechanism for anti-stalking of AirTags.

6.2 Reflections

This challenging project was an avenue for me to obtain new knowledge and gain or improve skills. I learnt a lot about the processes involved in the entire Bluetooth and BLE connectivity processes. The process of creating, sampling and testing a dataset was a theory I discovered too. Furthermore, I learnt more concepts in statistics and linear regression modelling despite my computer engineering background. My mind was opened to more techniques in the use of Kotlin programming language and in Android App development in general, hence my skills in the design and implementation of object-oriented programing were improved.

The project also made me realise how essential planning and time management were especially when I was briefly stuck on a way to run a build of the application. Good planning could have

prevented that vital time loss and also to position myself strategically for that unexpected expenditure at that time.

If I had to redo this project again with the knowledge I gained, I would manage my time better to produce a significant milestone relatively earlier so that more experimentation could be done on many specific scenarios and analysed carefully to hopefully produce more meaningful results, as it was a phase which could do with more time.

6.3 Conclusions

6.3.1 Project Contributions

This project contributes to the body of knowledge by presenting a specific Identifying Token that can be used to distinctly identify an AirTag and was integrated into an Android Application to detect AirTags using BLE scanning. We showed with results from experiments that this system was able to detect AirTags with very high accuracy. We also presented an estimated Measured Power value for the AirTag using a Linear Regression Model which can be used to estimate distance between a receiver and an AirTag. However, we showed that the distance estimates are not always equal or very close to actual distances.

6.3.2 Recommendations for Future Work

Further work might be undertaken to determine if another Identifying Token can be derived or predicted for the AirTag. This will involve more experimentation on the AirTag and its advertising packet to get a clearer view on its structure and how it behaves and changes. Also, more work on signal strength of the AirTag in many different scenarios, and environments and distances could be performed to better evaluate a more accurate measured power for each scenario. In evaluating the measured power, thorough modelling such as using a Polynomial Regression Model could be explored for its prediction. More work on stalker scenarios especially in commuting situations could be experimented on and analysed to discern an appropriate time value, or set of values, where stalking can be ascertained. Also, work could be done to implement an iOS version of the system to work on iPhones and iPads. Finally, more work on verification and validation could be done using a large number of BLE devices so as to check the reliability of the results illustrated in this report.

References

A. Barua, M. A. Al Alamin, M. S. Hossain and E. Hossain, "Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey," in IEEE Open Journal of the Communications Society, vol. 3, pp. 251-281, 2022, doi: 10.1109/OJCOMS.2022.3149732.

Adafruit.com. 2022. *Introduction to Bluetooth Low Energy*. [online] Available at: <https://learn.adafruit.com/introduction-to-bluetooth-low-energy/gap>

Adjei, H., Oduro-Gyimah, F., Shunhua, T., Agordzo, G. and Musariri, M., 2020. Developing a Bluetooth Based Tracking System for Tracking Devices Using Arduino. *2020 5th International Conference on Computing, Communication and Security (ICCCS)*

Ahmed, M., Hoque, M. and Khattak, A., 2016. Demo: Real-time vehicle movement tracking on Android devices through Bluetooth communication with DSRC devices. *2016 IEEE Vehicular Networking Conference (VNC).*

Amaldev, 2021. *UWB: The Tech Behind Apple AirTags - The Tech Blog*. [online] The Tech Blog. Available at: <http://amaldev.blog/uwb-the-tech-behind-apple-airtags/>

Android Developers. 2022. *android.bluetooth.le | Android Developers*. [online] Available at: <https://developer.android.com/reference/kotlin/android/bluetooth/le/package-summary>

Android Developers. 2022. *BluetoothLeScanner | Android Developers*. [online] Available at: <https://developer.android.com/reference/kotlin/android/bluetooth/le/BluetoothLeScanner>

Android Developers. 2022. *Kotlin and Android | Android Developers*. [online] Available at: <https://developer.android.com/kotlin>

Android Developers. 2022. *Notifications Overview | Android Developers*. [online] Available at: <https://developer.android.com/develop/ui/views/notifications>

Android Developers. 2022. *ScanFilter | Android Developers*. [online] Available at: <https://developer.android.com/reference/kotlin/android/bluetooth/le/ScanFilter>

REFERENCES

Android Developers. 2022. *ScanFilter.Builder | Android Developers*. [online] Available at: <https://developer.android.com/reference/kotlin/android/bluetooth/le/ScanFilter.Builder>

Android Developers. 2022. *ScanRecord | Android Developers*. [online] Available at: <https://developer.android.com/reference/kotlin/android/bluetooth/le/ScanRecord>

Android Developers. 2022. *ScanResult | Android Developers*. [online] Available at: <https://developer.android.com/reference/kotlin/android/bluetooth/le/ScanResult>

Android Developers. 2022. *ScanSettings | Android Developers*. [online] Available at: <https://developer.android.com/reference/kotlin/android/bluetooth/le/ScanSettings>

Apple (United Kingdom). 2020. *AirTag*. [online] Available at: <https://www.apple.com/uk/airtag/>

Becker, J., Li, D. and Starobinski, D., 2019. Tracking Anonymized Bluetooth Devices. *Proceedings on Privacy Enhancing Technologies*, 2019(3), pp.50-65.

Bluetooth® Technology Website. 2022. *Bluetooth Technology Overview | Bluetooth® Technology Website*. [online] Available at: <https://www.bluetooth.com/learn-about-bluetooth/tech-overview/>

Catley, A., 2022. *Apple AirTag Reverse Engineering - Adam Catley*. [online] Adamcatley.com. Available at: <https://adamcatley.com/AirTag.html>

Clover, J., 2022. *AirTags: Apple's Item Trackers - Everything We Know*. [online] MacRumors. Available at: <https://www.macrumors.com/guide/airtags/>

Clover, J., Hardwick, T., Charlton, H., Fathi, S. and Rossignol, J., 2021. *Apple Enhancing AirTags Anti-Stalking Measures With Android App and Shorter Sound Intervals*. [online] MacRumors. Available at: <https://www.macrumors.com/2021/06/03/apple-airtags-anti-stalking-measures/>

CNN. 2020. *Watch AirTag Apple event announcement - CNN Video*. [online] Available at: <https://edition.cnn.com/videos/business/2021/04/20/airtag-apple-announcement-orig.cnn-business>

Curry, D., 2022. *Apple Statistics (2022)*. [online] Business of Apps. Available at: <https://www.businessofapps.com/data/apple-statistics/>

REFERENCES

Digital Matter Support. 2020. *Active vs Passive Bluetooth® Scanning*. [online] Available at: <https://support.digitalmatter.com/support/solutions/articles/16000100684-active-vs-passive-bluetooth-scanning>

Estimote.com. 2022. [online] Available at: <https://community.estimote.com/hc/en-us/articles/201636913-What-are-Broadcasting-Power-RSSI-and-other-characteristics-of-a-beacon-s-signal->

fccid.io. 2022. [online] Available at: <https://fccid.io/document.php?id=5130965>

Gad, A., 2022. *Accuracy, Precision, and Recall in Deep Learning | Paperspace Blog*. [online] Paperspace Blog. Available at: <https://blog.paperspace.com/deep-learning-metrics-precision-recall-accuracy/#:~:text=Accuracy%20is%20a%20metric%20that,the%20total%20number%20of%20predictions.>

H. Kikuchi and T. Yokomizo, "Location Privacy Vulnerable from Bluetooth Devices," 2013 16th International Conference on Network-Based Information Systems, 2013, pp. 534-538,.

Hernandez-Solana, A., Perez-Diaz-De-Cerio, D., Valdovinos, A. and Valenzuela, J., 2018. Anti-Collision Adaptations of BLE Active Scanning for Dense IoT Tracking Applications. IEEE Access, 6, pp.53620-53637

Kim, H., Lim, J., Hong, W., Park, J., Kim, Y., Kim, M. and Lee, Y., 2019. Design of a Low-Power BLE5-Based Wearable Device for Tracking Movements of Football Players. *2019 International SoC Design Conference (ISOCC).*

Mac, R. and Hill, K., 2021. *Are Apple AirTags Being Used to Track People and Steal Cars?*. [online] Nytimes.com. Available at: <https://www.nytimes.com/2021/12/30/technology/apple-airtags-tracking-stalking.html>

Matei, A., 2022. *'I was just really scared': Apple AirTags lead to stalking complaints*. [online] the Guardian. Available at: <https://www.theguardian.com/technology/2022/jan/20/apple-airtags-stalking-complaints-technology>

REFERENCES

Md Isa, M., Abdul Jamil, M., Tengku Ibrahim, T., Ahmad, M., Abd Rahman, N. and Adon, M., 2019. Children Security and Tracking System Using Bluetooth and GPS Technology. *2019 9th IEEE International Conference on Control System, Computing and Engineering (ICCSCE).*

Mearian, L., 2019. *Ultra Wideband (UWB) explained (and why it's in the iPhone 11)*. [online] Computerworld. Available at: <https://www.computerworld.com/article/3490037/ultra-wideband-explained-and-why-its-in-the-iphone-11.html>

Mehrotra, S., 2021. *Apple launches AirTag for Android: How to find nearby AirTags using a smartphone?*. [online] Republic World. Available at: <https://www.republicworld.com/technology-news/how-to/apple-launches-airtag-for-android-how-to-find-nearby-airtags-using-a-smartphone.html>

Oram, A., 2022. *Here's how to use Apple's Tracker Detect Android app to find nearby AirTags*. [online] iMore. Available at: <https://www.imore.com/how-use-apple-tracker-detect-android>

Ponciano, J., 2022. *The World's Largest Tech Companies In 2022: Apple Still Dominates as Brutal Market Selloff Wipes Trillions In Market Value*. [online] Forbes. Available at: <https://www.forbes.com/sites/jonathanponciano/2022/05/12/the-worlds-largest-technology-companies-in-2022-apple-still-dominates-as-brutal-market-selloff-wipes-trillions-in-market-value/?sh=a26f49534488>

Pykes, K., 2020. *Oversampling and Undersampling*. [online] Medium. Available at: <https://towardsdatascience.com/oversampling-and-undersampling-5e2bbaf56dcf>

Ramos, A., Lazaro, A., Girbau, D. and Villarino, R., 2016. Introduction to RFID and Chipless RFID. *RFID and Wireless Sensors Using Ultra-Wideband Technology*, pp.1-18.

Riyas, M., 2022. *BLE-An overview.* [online] Medium. Available at: <https://medium.com/@muhamed.riyas/ble-an-overview-d524ceb73c94>

Shah, R., 2022. *Convert RSSI Value of the BLE (Bluetooth Low Energy) Beacons to Meters*. [online] Medium. Available at: <https://medium.com/beingcoders/convert-rssi-value-of-the-ble-bluetooth-low-energy-beacons-to-meters-63259f307283>

Silicon labs. 2022. [online] Available at: <https://docs.silabs.com/bluetooth/2.13/code-examples/stack-features/adv-and-scanning/adv-manufacturer-specific-data>

REFERENCES

Statology. 2022. *Understanding Heteroscedasticity in Regression Analysis - Statology*. [online] Available at: <https://www.statology.org/heteroscedasticity-regression/>

Warren, T., 2022. [online] Verge. Available at: <https://www.theverge.com/2022/1/28/22906071/apple-1-8-billion-active-devices-stats>

Appendix A

Project Proposal

APPENDICES

Design and Implementation of an Anti-Stalking System for Air Tags

1. Introduction

1.1. Problem

From the dawn of the past decade, Apple Inc. have developed and released many devices that have revolutionized the world of technology we live in now, mainly with the release of the iPhone, their flagship mobile device. Apple, with their focus on users having an ecosystem of their devices have developed and released many other personal products that work with their iPhone. These are the iPad, AirPods, Apple TV, HomePods, iPod Touch, the Apple Watch and the AirTags. (reuters.com, 2022)

The AirTags are tracking devices with the aim of enabling users to keep track of personal belongings, such as keys, your backpack, or other apple devices (AirTag, 2022). They are synced usually with the iPhone, by using the Find My App, thus allowing users to track the location of the AirTags, and by proxy the items they are attached to, at all times. Some of the items include keys, wallets, purses, backpacks, luggage and medical kits (Apple Newsroom, 2022). However, because of this tracking capability malicious users can use them for entirely different things they are supposed to be utilized for, as a result mainly leading to victims losing valuable property.

The AirTag is a relatively easily concealable device owing to its size, and when placed strategically on items to be tracked, malicious users are able to do so without being caught. There are reported cases of AirTags being used to track luxury cars, luxury belongings, and people's homes all unknowingly (nytimes.com, 2022). On cars, they are placed at an obscure spot with the owner oblivious to being tracked. This raises a huge concern for safety, privacy and security of every individual.

Currently, the measures Apple have put in place to prevent dubious tracking are far from enough (Clover et al., 2022). AirTags play sounds at a random time in a window within eight to twenty-four hours after being away from their owner. This is to alert the victim being tracked of supposed tracking by the AirTags, however this mechanism is not close to sufficient. At least 8 hours is enough time for a perpetrator to perform their actions. To buttress this point, the counter restarts when the AirTags come into contact with the owner, which means a stalker can prevent an alert from the AirTags if they plan accordingly. Also, the sound played by the AirTags is a 15 second loud chirping that can be missed by the victim. There are alerts given on iPhones in case of suspected stalking, but these alerts are not reliable and frequent enough. On Android phones however, Apple released an app called "TrackerScan" that enables Android Users to manually scan for trackers near them by informing the user or playing a sound on the AirTag (republic world.com, 2022) but this mechanism is also not adequate mainly due to the manual nature of detection.

Therefore, there is the pertinent need for active and proactive detection of AirTags when they are used maliciously for stalking since current measures are not enough. A reliable mechanism to detect the possibility of stalking by AirTags and inform victims timely is urgently needed. The main idea of this project is to detect possible stalking of AirTags automatically and alert possible victims timely.

1.2. Purpose of the Project

The purpose of this project is to design and implement an anti-stalking system for AirTags and other similar devices by leveraging Bluetooth Low Energy (BLE) technology. AirTags and other Bluetooth devices use advertising channels during Bluetooth connections to announce their presence, and this can enable a passive attack on them. Such devices however normally use periodically changing randomized address instead of their permanent Media Access Control (MAC) address as their advertising address to announce their presence (Becker, Li and Starobinski, 2019). One of the main challenges of the project is to derive Identifying Tokens or characteristics which can be extracted from the payload to detect accurately which particular device is doing the Bluetooth advertising. In effect, the idea is to identify when an AirTag is nearby and then to give an alert to the victim if stalking is suspected.

1.3. Aims

- We plan to design and implement an anti-stalking mobile application for AirTags which detects potential stalking and then alerts the user through pushing notifications

1.4. Objectives

- We will experiment with AirTags and other BLE devices to derive their respective exclusive Identifying Tokens to correctly detect them with a passive attack
- We plan to design a mobile application for detecting potential AirTag stalking which alerts timely
- We will implement the application for Android smart phones
- We will design and implement a notification alerting system for the mobile application system
- We intend to test if the system can adequately differentiate AirTags/trackers from other normal Bluetooth devices
- We will analyse the results to verify the accuracy in detecting potential stalking events
- We will base this project on previous works and techniques on Bluetooth tracking and detection

1.5. Research Question

The research question that we intend to answer is: “How to design and implement an anti-stalking system for AirTags?”

1.6. Products of the work

The product of the work is a mechanism that adequately detects AirTag tracking through passive attacks while differentiating it from other normal Bluetooth devices and connections in the form of s mobile application. The detection component of the proposed system and the alert component of the system will be implemented on the same mobile application. These two major components on the same mobile application form the products of the work.

1.7. Beneficiaries

The main beneficiaries of the project would be every user in the world who wants privacy, safety and security for themselves and their properties from malicious attackers.

Manufacturers involved in making and selling of anti-stalking schemes will benefit from this proposed project too.

This project could also be beneficial to other researchers who would like to tackle further work in anti-stalking and tracking using Bluetooth technology.

1.8. Project Scope

While tracking may be done using many forms of devices, work will be focused primarily on AirTags and secondarily on similar devices. Hence, most experimentation will be done with AirTags.

The work will mainly focus on tracking events related to transportation situations, i.e., while a potential victim is on a bus, a train or a personal vehicle going to a destination. As a result, design, implementation and testing will be done using these scenarios.

2. Critical Context/Literature Review

2.1. Introduction

Many devices today take advantage of Bluetooth Low Energy (BLE) to perform many critical functions remotely, especially with the advent of the Internet of Things (IOT) Space. Tracking using BLE powered devices like the AirTag are some of the important usages in today's world. However, it is also vital to make sure tracking is done in the right way to prevent or mitigate harm. So far, a lot of research has been done to track devices using Bluetooth (Adjei et al., 2020), (Ahmed et al., 2016) or even people of interest using Bluetooth (Kim et al., 2019), (Isa et al., 2019), but little focus has been put on tracking these Bluetooth devices that track other devices themselves.

With the premise of anti-tracking however, research has shown that Bluetooth devices can be passively monitored and tracked even with modern devices employing anonymizing measures to prevent tracking (Becker, Li and Starobinski, 2019). Also, other research illustrated how Bluetooth powered devices can discover a large number of devices in high density scenarios during active scanning (Hernandez-Solana et al., 2018).

Privacy of individuals and their belongings is something that is easily compromised with the onset of tracking. Lack of Privacy is one of the key banes of Bluetooth Technology these days and hence research on this topic was explored.

2.2. Tracking Anonymized Bluetooth Devices

(Becker, Li and Starobinski, 2019) presented an address-carryover algorithm that exploited the asynchronous nature of payload and address changes in BLE devices to achieve tracking of these devices beyond their address randomization cycles. As briefly mentioned earlier, BLE powered devices announce their presence by advertising on non-encrypted public channels, and hence to prevent tracking on these channels, they employ the use of periodically changing random addresses to thwart off trackers. This research illustrated an effective way of passively monitoring these devices. They also presented an identity-exposing attack that allowed permanent non-continuous tracking of BLE devices. The techniques and algorithms shown by this work will be leveraged in the tracking of AirTags and other similar BLE-enabled tracking devices.

2.3. Discovering Many Devices in High Density Scenarios

Here, the authors (Hernandez-Solana et al., 2018) analysed backoff in Neighbour discovery process (NDP) of BLE and proposed a simple and practical adaptation of algorithm on scanner functionality. Together with a new proposed back off scheme, the discovery latencies of BLE devices were improved, and led to high probability of discovering a large number of devices in high density situations. Work from here is also important in helping to improve the success rate of finding supposed AirTags in places which may have a lot of Bluetooth devices, typically trains or other public transport.

2.4. Tracking Other Devices/Persons of Interest Using Bluetooth

(Adjei et al., 2020) discussed and analysed an Arduino based device which was designed to track and monitor valuable items that a user wanted monitored within a range of 10 meters at all times in real-time. A unique approach used was the use of Bluetooth for connection between the user's phone and the Arduino device. The results of the experiment were able to show that as soon as connection is lost, a call was made from the device to the user's phone to signal a disconnection, and an alert message containing the current location was sent via Global System for Mobile Communications (GSM). They were also able to demonstrate that after every 1000milliseconds, updated coordinates were sent to the user, assisting in tracking the device even if its location had changed.

(Ahmed et al., 2016) described an Android application used for the visualization of real-time vehicle movements on Google map using Dedicated Short-Range Communication (DSRC) and Bluetooth communication. The android application communicated with one of the DSRC units through Bluetooth to gather real-time traces collected from all DSRC-equipped vehicles. The application then displayed live movement of these vehicles on Google map with their path history, speed and direction.

(Kim et al., 2019) Presented a prototype wearable device that tracked movements of football players during the match time. The acquired data was transferred from the device using Bluetooth Low Energy (BLE) protocol. The experimental results showed that the BLE-based wearable device successfully illustrated the real-time tracking operation, achieving the low-power solution compared to the existing devices.

To address cases of missing children that have been springing up, (Isa et al., 2019) proposed a child tracking system to help parents monitor their kids in public spaces as a countermeasure to these situations. The device used the alarm technique, which triggers when

the Bluetooth connection is disconnected between the parent and the child. The GPS application was used to track the location of the supposed missing child wearing this device. The child detector device was made up of two main units, one for parents and the other for child. The child's unit functioned as a transmitter which transmitted a GPS signal, while the parent's unit received the signal, and worked with their smartphone to determine the position and distance of their child.

2.5. Privacy

(Kikuchi et al., 2013) reported the experimental results on scanning Mac address of Bluetooth devices and showed the risk of location privacy to be compromised from the Bluetooth scanning. Focus was on this work because Bluetooth is a wireless network protocol widely used for many mobile devices, and by individuals possessing them, they were at risk of being identified without noticing.

(Albazrqaoe et al., 2019) presented a practical Bluetooth traffic sniffer called BlueEar. which featured a novel dual-radio architecture where two Bluetooth-compliant radios coordinated with each other on learning the hopping sequence of indiscoverable Bluetooth networks, predicting adaptive hopping behavior, and mitigating the impacts of RF interference. Experiment results showed that BlueEar could maintain a packet capture rate higher than 90% consistently in real-world environments, where the target Bluetooth network exhibits diverse hopping behaviors in the presence of dynamic interference from coexisting 802.11 devices. Also, the authors discussed the privacy implications of the BlueEar system and presented a practical countermeasure that reduced the packet capture rate of the sniffer to 20%.

(Barua et al., 2022) focused on security vulnerabilities of the BLE protocol. They presented a comprehensive taxonomy for the security and privacy issues of BLE by presenting possible attack scenarios for different types of vulnerabilities, classifying them according to their severity, and listing possible mitigation techniques. They also provide case studies regarding how different vulnerabilities can be exploited in real BLE devices.

3. Approaches: Methods & Tools for Design, Analysis & Evaluation

3.1. Methods & Tools

3.1.1. Design

For this initial phase of the project, the basis of the work will be inspired from similar studies, proposals, theory and literature on app development with frameworks and APIs, and the extraction of Identifying Tokens or characteristics of Bluetooth Devices by using a Bluetooth Sniffer to observe Bluetooth packets. The work will also be based on former projects and proposals which involve building applications using software engineering process such as the Agile Method.

3.1.2. Implementation

In this phase of the project, BLE advertising packets of AirTags will be analysed using a Bluetooth Sniffer to extract the suitable Identifying Token for detecting AirTags. These experiments will be done and observed on a laptop. Code for a mobile application will be

programmed in Java with the Android API on a laptop using an IDE such as Android Studio. The server side of the mobile app which handles the detection and alerting algorithm will be implemented in Python with a framework such as FastAPI.

3.1.3. Analysis & Evaluation

To assess the efficiency and effectiveness of the implementation of the system, several tests will be run for evaluation of metrics including computational cost, computational time, false positives, accuracy of detection. The main tests to be done are:

- Test the ability of the system to identify AirTags by using derived Identifying Tokens to identify nearby AirTags
- Test the accuracy of the system in detecting AirTags from a crowd of many Bluetooth devices
- Test the accuracy of the system in detecting potential tracking scenarios with AirTags by simulating various scenarios of stalking and using the built mobile application to respectively detect them
- Test whether the alert component of the mobile application is accurate by evaluating accuracy of alert events

3.2. Ethical, Legal and Professional Issues

As declared in the Research Ethics Review Form, no human participant contributions are needed in this project. The work will involve articles, journals, studies and other online resources such as source codes, algorithms, video tutorials allowed to be used in this project, and will be properly referenced to avoid committing plagiarism

4. Work Plan

4.1. Dependencies

In order to derive a good design for the project, a lot of research in literature and available online materials will be consulted. The ideas and knowledge obtained there will enlighten the suitable techniques and skills needed for that phase of the project. Also, tutorials and documentations of all the resources needed such as programming language and IDEs will help in the implementation phase of the project.

The testing of the identifying Tokens for AirTags will be done in the implementation phase to be sure that the alert component of system will function as it is supposed to. The implementation of the Detection Component of the system will overlap with this testing as well as the implementation of the Alert Component.

For the analysis and evaluation phase, these tests are intended to be independent of each other hence there is no specific order they are set in. They will be tested in parallel as shown in the Gantt chart (Fig 1).

APPENDICES

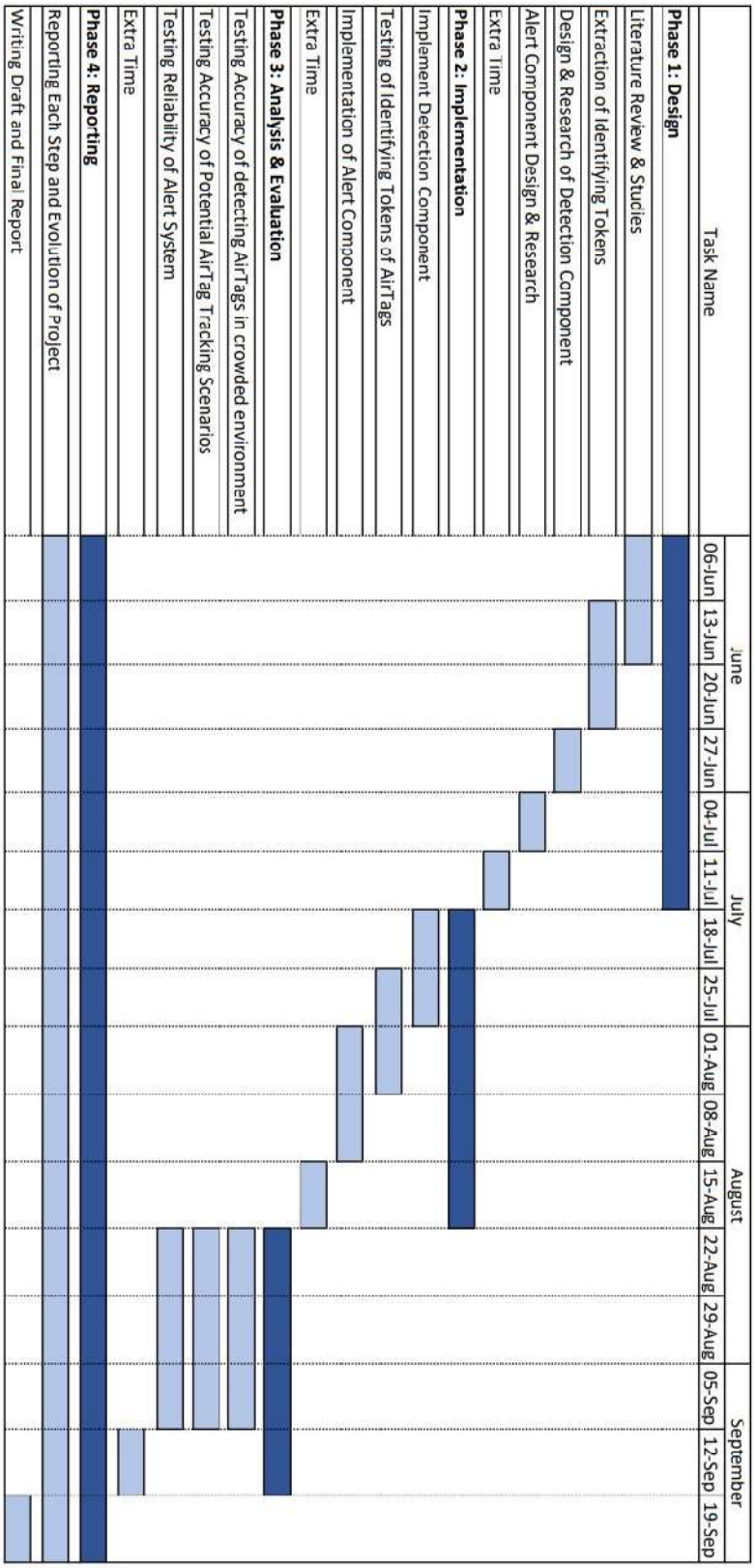

Fig 1. Gantt Chart

4.2. Time Allocation

The first phase, the Design, is the part with which more focus will be put into since a lot of learning and research about the project is done there, as well as the unknown factors that come along with it. This phase has more focus as compared to the implementation phase because implementation will be easier and straightforward when a solid design and plan is made. With the amount of educational material online pertaining to Bluetooth technology and mobile app development, there is a lot of aid in the implementation phase. A background in programming also helps.

4.3. Reporting and Meetings

Reporting every milestone achievement will be done during the entirety of the whole project allocated time. This helps keep a detailed record of the work being done and also ease the documentation of the final dissertation report.

Meetings with the supervisor will be arranged after a major milestone has been completed to summarize what has been done and to discuss tasks needed to be completed. Meetings will also be arranged for clarification purposes or for advice when problems arise.

5. Risks

Risk	Likelihood (1-3)	Consequences (1-5)	Impact (L x C)	Mitigation Strategy
Lack of skill or understanding about theories or tools	1	3	3	Learn more tutorials, read more documents or seek assistance
Loss of Data	2	4	8	Frequent backup of data on an external medium such as the cloud
Identifying Tokens cannot be extracted	2	5	10	Simulated Theoretical Values can be used instead at least
Some tasks need more time than expected	2	5	10	Three weeks of extra time have been allocated in the case that some is needed as shown on the Gantt chart
Code is lost, overwritten or changes have made it unstable	3	5	15	An online tool like GitHub will be used to provide backup and version control for codes

APPENDICES

References

reuters.com. 2022. [online] Available at: <https://www.reuters.com/companies/AAPL.O>.

Apple (United Kingdom). 2022. *AirTag*. [online] Available at: <https://www.apple.com/uk/airtag/> .

Apple Newsroom. 2022. *An update on AirTag and unwanted tracking*. [online] Available at: <https://www.apple.com/newsroom/2022/02/an-update-on-airtag-and-unwanted-tracking/>.

Nytimes.com. 2022. *Are Apple AirTags Being Used to Track People and Steal Cars?*. [online] Available at: <https://www.nytimes.com/2021/12/30/technology/apple-airtags-tracking-stalking>.

Clover, J., Charlton, H., Hardwick, T., Fathi, S. and Staff, M., 2022. *Apple Enhancing AirTags Anti-Stalking Measures With Android App and Shorter Sound Intervals*. [online] MacRumors. Available at: <https://www.macrumors.com/2021/06/03/apple-airtags-anti-stalking-measures/>.

Republic World. 2022. *Apple launches AirTag for Android: How to find nearby AirTags using a smartphone?*. [online] Available at: <https://www.republicworld.com/technology-news/how-to/apple-launches-airtag-for-android-how-to-find-nearby-airtags-using-a-smartphone.html>

Becker, J., Li, D. and Starobinski, D., 2019. Tracking Anonymized Bluetooth Devices. *Proceedings on Privacy Enhancing Technologies*, 2019(3), pp.50-65.

Adjei, H., Oduro-Gyimah, F., Shunhua, T., Agordzo, G. and Musariri, M., 2020. Developing a Bluetooth Based Tracking System for Tracking Devices Using Arduino. *2020 5th International Conference on Computing, Communication and Security (ICCCS)*,.

Ahmed, M., Hoque, M. and Khattak, A., 2016. Demo: Real-time vehicle movement tracking on Android devices through Bluetooth communication with DSRC devices. *2016 IEEE Vehicular Networking Conference (VNC)*,.

Kim, H., Lim, J., Hong, W., Park, J., Kim, Y., Kim, M. and Lee, Y., 2019. Design of a Low-Power BLE5-Based Wearable Device for Tracking Movements of Football Players. *2019 International SoC Design Conference (ISOCC)*,.

Md Isa, M., Abdul Jamil, M., Tengku Ibrahim, T., Ahmad, M., Abd Rahman, N. and Adon, M., 2019. Children Security and Tracking System Using Bluetooth and GPS Technology. *2019 9th IEEE International Conference on Control System, Computing and Engineering (ICCSCE)*,.

Hernandez-Solana, A., Perez-Diaz-De-Cerio, D., Valdovinos, A. and Valenzuela, J., 2018. Anti-Collision Adaptations of BLE Active Scanning for Dense IoT Tracking Applications. *IEEE Access*, 6, pp.53620-53637.

H. Kikuchi and T. Yokomizo, "Location Privacy Vulnerable from Bluetooth Devices," 2013 16th International Conference on Network-Based Information Systems, 2013, pp. 534-538,.

W. Albazrqaoe, J. Huang and G. Xing, "A Practical Bluetooth Traffic Sniffing System: Design, Implementation, and Countermeasure," in IEEE/ACM Transactions on Networking, vol. 27, no. 1, pp. 71-84, Feb. 2019, doi: 10.1109/TNET.2018.2880970.

A. Barua, M. A. Al Alamin, M. S. Hossain and E. Hossain, "Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey," in IEEE Open Journal of the Communications Society, vol. 3, pp. 251-281, 2022, doi: 10.1109/OJCOMS.2022.3149732.

APPENDICES

Research Ethics Review Form: BSc, MSc and MA Projects

Computer Science Research Ethics Committee (CSREC)

A.1 If you answer YES to any of the questions in this block, you must apply to an appropriate external ethics committee for approval and log this approval as an External Application through Research Ethics Online - https://ethics.city.ac.uk/		
1.1	Does your research require approval from the National Research Ethics Service (NRES)? *e.g. because you are recruiting current NHS patients or staff?* *If you are unsure try - https://www.hra.nhs.uk/approvals-amendments/what-approvals-do-i-need/*	**NO**
1.2	Will you recruit participants who fall under the auspices of the Mental Capacity Act? *Such research needs to be approved by an external ethics committee such as NRES or the Social Care Research Ethics Committee - http://www.scie.org.uk/research/ethics-committee/*	**NO**
1.3	Will you recruit any participants who are currently under the auspices of the Criminal Justice System, for example, but not limited to, people on remand, prisoners and those on probation? *Such research needs to be authorised by the ethics approval system of the National Offender Management Service.*	**NO**
A.2 If you answer YES to any of the questions in this block, then unless you are applying to an external ethics committee, you must apply for approval from the Senate Research Ethics Committee (SREC) through Research Ethics Online - https://ethics.city.ac.uk/		
2.1	Does your research involve participants who are unable to give informed consent? *For example, but not limited to, people who may have a degree of learning disability or mental health problem, that means they are unable to make an informed decision on their own behalf.*	**NO**
2.2	Is there a risk that your research might lead to disclosures from participants concerning their involvement in illegal activities?	**NO**
2.3	Is there a risk that obscene and or illegal material may need to be accessed for your research study (including online content and other material)?	**NO**
2.4	Does your project involve participants disclosing information about special category or sensitive subjects? *For example, but not limited to: racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health; sexual life; criminal offences and proceedings*	**NO**
2.5	Does your research involve you travelling to another country outside of the UK, where the Foreign & Commonwealth Office has issued a travel warning that affects the area in which you will study?	**NO**

APPENDICES

	Please check the latest guidance from the FCO - http://www.fco.gov.uk/en/	
2.6	Does your research involve invasive or intrusive procedures? *These may include, but are not limited to, electrical stimulation, heat, cold or bruising.*	**NO**
2.7	Does your research involve animals?	**NO**
2.8	Does your research involve the administration of drugs, placebos or other substances to study participants?	**NO**
A.3 If you answer YES to any of the questions in this block, then unless you are applying to an external ethics committee or the SREC, you must apply for approval from the Computer Science Research Ethics Committee (CSREC) through Research Ethics Online - https://ethics.city.ac.uk/ **Depending on the level of risk associated with your application, it may be referred to the Senate Research Ethics Committee.**		
3.1	Does your research involve participants who are under the age of 18?	**NO**
3.2	Does your research involve adults who are vulnerable because of their social, psychological or medical circumstances (vulnerable adults)? *This includes adults with cognitive and / or learning disabilities, adults with physical disabilities and older people.*	**NO**
3.3	Are participants recruited because they are staff or students of City, University of London? *For example, students studying on a particular course or module.* *If yes, then approval is also required from the Head of Department or Programme Director.*	**NO**
3.4	Does your research involve intentional deception of participants?	**NO**
3.5	Does your research involve participants taking part without their informed consent?	**NO**
3.5	Is the risk posed to participants greater than that in normal working life?	**NO**
3.7	Is the risk posed to you, the researcher(s), greater than that in normal working life?	**NO**
A.4 If you answer YES to the following question and your answers to all other questions in sections A1, A2 and A3 are NO, then your project is deemed to be of MINIMAL RISK. **If this is the case, then you can apply for approval through your supervisor under PROPORTIONATE REVIEW. You do so by completing PART B of this form.** **If you have answered NO to all questions on this form, then your project does not require ethical approval. You should submit and retain this form as evidence of this.**		
4	Does your project involve human participants or their identifiable personal data? *For example, as interviewees, respondents to a survey or participants in testing.*	**NO**

Appendix B

Raw Results

APPENDICES

Experiments Dataset

EXP No,Flag,MAC Address,Advertising Data,Manufacturer Specific Data,SS at 0.02m,SS at 0.5m,SS at 1m,SS at 3m,SS at 5m,DM at 0.02m,DM at 0.5m,DM at 1m,DM at 3m,DM at 5m,Detected

1,0,D3:22:08:9D:6C:0C,0x1EFF4C00121910B7C647488AF528604D6DEDCB89EC467E80354F52FDEE00E1,0x121910B7C647488AF528604D6DEDCB89EC467E80354F52FDEE00E1,-21,-46,-53,-72,-81,0.258,1.542,3.017,4.358,4.47,Yes

2,0,CB:B9:85:97:68:98,0X1EFF4C001219108CA0E992D45396BF65CB03D41899079AE0DCC570E0C70208,0X1219108CA0E992D45396BF65CB03D41899079AE0DCC570E0C70208,-21,-49,-63,-71,-79,0.455,2.019,2.942,3.164,8.688,Yes

3,0,DB:2F:86:BF:09:8C,0X1EFF4C00121910F0B9551C79E23EED5298A6EC89AC9ECC0AD933856CAC0072,0X121910F0B9551C79E23EED5298A6EC89AC9ECC0AD933856CAC0072,-23,-48,-52,-70,-76,0.329,1.664,2.582,3.274,6.716,Yes

4,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

5,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

6,0,C6:56:4F:7B:F0:44,0X1EFF4C001219105075B0B2FCCBD399OF91D333573C8138100EF7F45BC60044,0X1219105075B0B2FCCBD399OF91D333573C8138100EF7F45BC60044,-24,-45,-52,-74,NA,0.369,0.889,2.449,2.635,NA,Yes

7,0,CB:18:6D:32:F8:56,0X1EFF4C0012191091F33832EC2211E0993000535DCCB99BEC2B04448EA10358,0X12191091F33832EC2211E0993000535DCCB99BEC2B04448EA10358,-27,-47,-56,-72,NA,0.236,1.452,1.939,3.928,NA,Yes

8,0,C6:56:4F:7B:F0:44,0X1EFF4C001219105075B0B2FCCBD399OF91D333573C8138100EF7F45BC600C5,0X1219105075B0B2FCCBD399OF91D333573C8138100EF7F45BC600C5,-26,-47,-59,-73,NA,0.363,1.974,1.871,2.125,NA,Yes

9,0,CB:18:6D:32:F8:56,0X1EFF4C0012191091F33832EC2211E0993000535DCCB99BEC2B04448EA10345,0X12191091F33832EC2211E0993000535DCCB99BEC2B04448EA10345,-21,-48,-52,-70,NA,0.313,1.109,2.202,4.784,NA,Yes

APPENDICES

10,0,C6:56:4F:7B:F0:44,0X1EFF4C001219105075B0B2FCCBD399OF91D333573C8138100EF7F45BC6001A,0X1219105075B0B2FCCBD399OF91D333573C8138100EF7F45BC6001A,-29,-48,-54,-72,NA,0.229,1.509,1.204,4.761,NA,Yes

11,0,CB:18:6D:32:F8:56,0X1EFF4C0012191091F33832EC2211E0993000535DCCB99BEC2B04448EA10351,0X12191091F33832EC2211E0993000535DCCB99BEC2B04448EA10351,-23,-49,-63,-70,NA,0.28,1.565,2.456,5.092,NA,Yes

12,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

13,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

14,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

15,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

16,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

17,0,F7:BE:E6:60:50:AE,0X1EFF4C001219107CD53ECAB5666265A7C7135255A04CDE2C36B2279B1102AE,0X1219107CD53ECAB5666265A7C7135255A04CDE2C36B2279B1102AE,-21,-49,-53,-70,-81,0.339,1.534,1.739,3.065,6.603,Yes

18,0,FD:F3:C9:39:0A:BD,0X1EFF4C001219101FA80E13E51519767E677A59A61C94626B2BBB2454AF03BD,0X1219101FA80E13E51519767E677A59A61C94626B2BBB2454AF03BD,-24,-48,-59,-74,-83,0.47,0.815,2.855,4.811,6.881,Yes

19,0,F7:BE:E6:60:50:AE,0X1EFF4C001219107CD53ECAB5666265A7C7135255A04CDE2C36B2279B110262,0X1219107CD53ECAB5666265A7C7135255A04CDE2C36B2279B110262,-22,-49,-56,-74,-84,0.217,0.829,2.103,4.834,5.48,Yes

20,0,FD:F3:C9:39:0A:BD,0X1EFF4C001219101FA80E13E51519767E677A59A61C94626B2BBB2454AF037D,0X1219101FA80E13E51519767E677A59A61C94626B2BBB2454AF037D,-25,-46,-58,-72,-78,0.396,1.033,1.2,4.482,7.788,Yes

21,1,F7:BE:E6:60:50:AE,0X1EFF4C001219107CD53ECAB5666265A7C7135255A04CDE2C36B2279B110262,0X1219107CD53ECAB5666265A7C7135255A04CDE2C36B2279B110262,-23,-48,-58,-74,-76,0.402,0.736,0.967,2.08,5.778,Yes

22,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

APPENDICES

23,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

24,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

25,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

26,0,EE:B0:7B:28:93:19,0X1EFF4C001219104488D3861BFBB2FFB2889CD13FAE58699096D07423980019,0X1219104488D3861BFBB2FFB2889CD13FAE58699096D07423980019,-21,-45,-61,-71,NA,0.309,0.878,1.528,5.194,NA,Yes

27,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,Yes

28,0,DA:A9:07:B4:20:DC,0X1EFF4C00121910B50BE2307B22FABB73DCD9FFBA6740527943E13C49A9023C,0X121910B50BE2307B22FABB73DCD9FFBA6740527943E13C49A9023C,-26,-45,-57,-70,NA,0.411,1.973,2.363,3.675,NA,Yes

29,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

30,0,EE:B0:7B:28:93:19,0X1EFF4C001219104488D3861BFBB2FFB2889CD13FAE58699096D07423980049,0X1219104488D3861BFBB2FFB2889CD13FAE58699096D07423980049,-24,-48,-53,-71,NA,0.42,0.744,2.098,4.735,NA,Yes

31,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

32,0,EE:B0:7B:28:93:19,0X1EFF4C001219104488D3861BFBB2FFB2889CD13FAE58699096D07423980043,0X1219104488D3861BFBB2FFB2889CD13FAE58699096D07423980043,-24,-49,-52,-74,NA,0.332,1.665,1.866,2.895,NA,Yes

33,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

34,0,DA:A9:07:B4:20:DC,0X1EFF4C00121910B50BE2307B22FABB73DCD9FFBA6740527943E13C49A90228,0X121910B50BE2307B22FABB73DCD9FFBA6740527943E13C49A90228,-24,-45,-53,-71,NA,0.337,0.973,2.397,2.279,NA,Yes

35,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

36,0,EE:B0:7B:28:93:19,0X1EFF4C001219104488D3861BFBB2FFB2889CD13FAE58699096D07423980043,0X1219104488D3861BFBB2FFB2889CD13FAE58699096D07423980043,-23,-48,-52,-72,NA,0.258,0.969,2.266,4.163,NA,Yes

APPENDICES

37,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

38,0,EE:B0:7B:28:93:19,0X1EFF4C001219104488D3861BFBB2FFB2889CD13FAE58699096D07423980043,0X1219104488D3861BFBB2FFB2889CD13FAE58699096D07423980043,-23,-48,-58,-70,NA,0.415,0.85,1.634,3.817,NA,Yes

39,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

40,0,EE:B0:7B:28:93:19,0X1EFF4C001219104488D3861BFBB2FFB2889CD13FAE58699096D07423980043,0X1219104488D3861BFBB2FFB2889CD13FAE58699096D07423980043,-24,-49,-56,-72,NA,0.257,1.438,2.98,2.837,NA,Yes

41,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

42,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

43,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

44,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

45,0,DA:A9:07:B4:20:DC,0X1EFF4C00121910B50BE2307B22FABB73DCD9FFBA6740527943E13C49A90228,0X121910B50BE2307B22FABB73DCD9FFBA6740527943E13C49A90228,-24,-46,-63,-72,-82,0.484,1.772,2.698,3.055,5.558,Yes

46,0,DA:A9:07:B4:20:DC,0X1EFF4C00121910B50BE2307B22FABB73DCD9FFBA6740527943E13C49A90228,0X121910B50BE2307B22FABB73DCD9FFBA6740527943E13C49A90228,-27,-49,-57,-74,-78,0.423,0.88,1.638,4.279,4.971,Yes

47,0,DA:A9:07:B4:20:DC,0X1EFF4C00121910B50BE2307B22FABB73DCD9FFBA6740527943E13C49A90228,0X121910B50BE2307B22FABB73DCD9FFBA6740527943E13C49A90228,-23,-46,-63,-74,-81,0.346,1.358,1.033,4.351,5.628,Yes

48,0,DA:A9:07:B4:20:DC,0X1EFF4C00121910B50BE2307B22FABB73DCD9FFBA6740527943E13C49A90228,0X121910B50BE2307B22FABB73DCD9FFBA6740527943E13C49A90228,-22,-49,-56,-71,-84,0.214,1.807,2.619,5.275,4.463,Yes

49,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

50,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

APPENDICES

51,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

52,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

53,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

54,0,EC:A4:CE:3D:E0:A8,0X1EFF4C00121910DF7D90E4A791636526DCD79DD488F6795F10CC126E3C01A8,0X121910DF7D90E4A791636526DCD79DD488F6795F10CC126E3C01A8,-24,-47,-63,-71,NA,0.237,1.889,3.04,4.478,NA,Yes

55,0,D1:E1:3D:93:60:34,0X1EFF4C0012191055A816F1DBF2F7FADC2CD18988F8C18E478CB7EA73AD0034,0X12191055A816F1DBF2F7FADC2CD18988F8C18E478CB7EA73AD0034,-23,-45,-62,-71,NA,0.284,0.796,2.833,4.198,NA,Yes

56,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

57,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

58,0,EC:A4:CE:3D:E0:A8,0X1EFF4C00121910DF7D90E4A791636526DCD79DD488F6795F10CC126E3C01A8,0X121910DF7D90E4A791636526DCD79DD488F6795F10CC126E3C01A8,-22,-45,-53,-73,-80,0.418,1.364,2.316,2.498,6.784,Yes

59,0,D1:E1:3D:93:60:34,0X1EFF4C0012191055A816F1DBF2F7FADC2CD18988F8C18E478CB7EA73AD0034,0X12191055A816F1DBF2F7FADC2CD18988F8C18E478CB7EA73AD0034,-22,-47,-58,-73,-76,0.405,1.879,2.219,5.009,8.376,Yes

60,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

61,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

62,0,FA:AB:29:CE:49:73,0X1EFF4C00121910F82B595636E9D4D13BE96844D16AED8DF02A27ABA9C10273,0X121910F82B595636E9D4D13BE96844D16AED8DF02A27ABA9C10273,-24,-47,-57,-71,-80,0.479,1.629,3.038,3.312,4.337,Yes

63,0,E0:3A:2C:C9:2E:FD,0X1EFF4C001219105CB4F25D26DF1C0B87ADEA40EF545BE380168F7E780003FD,0X1219105CB4F25D26DF1C0B87ADEA40EF545BE380168F7E780003FD,-23,-46,-62,-73,-82,0.315,1.827,1.349,5.066,7.833,Yes

64,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

APPENDICES

65,0,FA:AB:29:CE:49:73,0X1EFF4C00121910F82B595636E9D4D13BE96844D16AED8DF02A27ABA9C1026B,0X121910F82B595636E9D4D13BE96844D16AED8DF02A27ABA9C1026B,-25,-47,-63,-70,-80,0.272,1.553,1.622,2.092,8.103,Yes

66,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

67,0,E0:3A:2C:C9:2E:FD,0X1EFF4C001219105CB4F25D26DF1C0B87ADEA40EF545BE380168F7E7800032F,0X1219105CB4F25D26DF1C0B87ADEA40EF545BE380168F7E7800032F,-23,-48,-61,-74,-83,0.337,0.896,1.17,2.142,4.632,Yes

68,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

69,0,FA:AB:29:CE:49:73,0X1EFF4C00121910F82B595636E9D4D13BE96844D16AED8DF02A27ABA9C1024A,0X121910F82B595636E9D4D13BE96844D16AED8DF02A27ABA9C1024A,-23,-48,-59,-71,-84,0.333,1.355,2.009,3.511,4.986,Yes

70,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

71,0,E0:3A:2C:C9:2E:FD,0X1EFF4C001219105CB4F25D26DF1C0B87ADEA40EF545BE380168F7E78000336,0X1219105CB4F25D26DF1C0B87ADEA40EF545BE380168F7E78000336,-25,-45,-52,-74,-76,0.386,0.913,0.94,5.032,7.242,Yes

72,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

73,0,FA:AB:29:CE:49:73,0X1EFF4C00121910F82B595636E9D4D13BE96844D16AED8DF02A27ABA9C102EA,0X121910F82B595636E9D4D13BE96844D16AED8DF02A27ABA9C102EA,-26,-48,-62,-71,-77,0.241,1.712,2.757,4.983,5.241,Yes

74,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

75,0,E0:3A:2C:C9:2E:FD,0X1EFF4C001219105CB4F25D26DF1C0B87ADEA40EF545BE380168F7E7800037B,0X1219105CB4F25D26DF1C0B87ADEA40EF545BE380168F7E7800037B,-25,-49,-59,-74,-80,0.498,1.432,2.291,3.228,6.114,Yes

76,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

77,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

78,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

APPENDICES

79,0,D3:BC:BA:3B:EE:8D,0X1EFF4C00121910D60B308E463F754B48B925AC19AE5FC58D8F9A90DDDF038D,0X121910D60B308E463F754B48B925AC19AE5FC58D8F9A90DDDF038D,-23,-45,-60,-71,NA,0.402,1.447,0.938,3.478,NA,Yes

80,0,D3:BC:BA:3B:EE:8D,0X1EFF4C00121910D60B308E463F754B48B925AC19AE5FC58D8F9A90DDDF038D,0X121910D60B308E463F754B48B925AC19AE5FC58D8F9A90DDDF038D,-24,-46,-58,-73,NA,0.456,1.494,1.64,4.419,NA,Yes

81,0,D3:BC:BA:3B:EE:8D,0X1EFF4C00121910D60B308E463F754B48B925AC19AE5FC58D8F9A90DDDF039C,0X121910D60B308E463F754B48B925AC19AE5FC58D8F9A90DDDF039C,-23,-49,-63,-71,NA,0.322,1.212,1.408,3.375,NA,Yes

82,0,D3:BC:BA:3B:EE:8D,0X1EFF4C00121910D60B308E463F754B48B925AC19AE5FC58D8F9A90DDDF039C,0X121910D60B308E463F754B48B925AC19AE5FC58D8F9A90DDDF039C,-23,-46,-53,-70,NA,0.258,1.628,1.738,3.88,NA,Yes

83,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

84,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

85,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

86,0,C8:24:BF:04:CE:6C,0X1EFF4C001219101D15008D34FF7391FE145837ACD3E4A69864579B8AB9016C,0X1219101D15008D34FF7391FE145837ACD3E4A69864579B8AB9016C,-25,-45,-52,-74,-81,0.478,1.886,2.93,4.869,4.946,Yes

87,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

88,0,C8:24:BF:04:CE:6C,0X1EFF4C001219101D15008D34FF7391FE145837ACD3E4A69864579B8AB9016C,0X1219101D15008D34FF7391FE145837ACD3E4A69864579B8AB9016C,-23,-48,-55,-71,-79,0.468,1.089,2.199,4.816,7.341,Yes

89,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

90,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

91,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

92,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

APPENDICES

93,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

94,0,DD:2A:12:99:8C:BD,0X1EFF4C00121910AA75126E6ADDF2EF8AA63A04031A047125E156B1D8D00BD,0X121910AA75126E6ADDF2EF8AA63A04031A047125E156B1D8D00BD,-29,-49,-55,-72,-84,0.401,0.85,2.259,5.189,7.29,Yes

95,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

96,0,DD:2A:12:99:8C:BD,0X1EFF4C00121910AA75126E6ADDF2EF8AA63A04031A047125E156B1D8D00BD,0X121910AA75126E6ADDF2EF8AA63A04031A047125E156B1D8D00BD,-27,-46,-55,-73,-80,0.404,1.133,2.854,2.759,4.99,Yes

97,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

98,0,C8:24:BF:04:CE:6C,0X1EFF4C001219101D15008D34FF7391FE145837ACD3E4A69864579B8AB9010D,0X1219101D15008D34FF7391FE145837ACD3E4A69864579B8AB9010D,-25,-47,-63,-70,NA,0.446,1.62,2.097,3.825,NA,Yes

99,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

100,0,DD:2A:12:99:8C:BD,0X1EFF4C00121910AA75126E6ADDF2EF8AA63A04031A047125E156B1D8D002F,0X121910AA75126E6ADDF2EF8AA63A04031A047125E156B1D8D002F,-27,-46,-63,-72,NA,0.398,1.215,1.032,3.98,NA,Yes

101,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

102,0,F8:0A:DA:33:07:BA,0X1EFF4C00121910EC932CEEC3ED5D9A5BC697F417E838463EDBC55F993701BA,0X121910EC932CEEC3ED5D9A5BC697F417E838463EDBC55F993701BA,-24,-49,-53,-74,-83,0.371,1.799,2.227,3.748,5.206,Yes

103,0,F8:0A:DA:33:07:BA,0X1EFF4C00121910EC932CEEC3ED5D9A5BC697F417E838463EDBC55F993701BA,0X121910EC932CEEC3ED5D9A5BC697F417E838463EDBC55F993701BA,-23,-45,-63,-70,-78,0.294,0.879,1.32,5.168,5.749,Yes

104,0,F8:0A:DA:33:07:BA,0X1EFF4C00121910EC932CEEC3ED5D9A5BC697F417E838463EDBC55F993701BA,0X121910EC932CEEC3ED5D9A5BC697F417E838463EDBC55F993701BA,-24,-48,-58,-73,-77,0.42,1.489,1.547,2.279,7.632,Yes

APPENDICES

105,0,F8:0A:DA:33:07:BA,0X1EFF4C00121910EC932CEEC3ED5D9A5BC697F417E838463EDBC55F99370136,0X121910EC932CEEC3ED5D9A5BC697F417E838463EDBC55F99370136,-25,-49,-60,-74,-78,0.213,0.814,2.156,2.624,5.071,Yes

106,0,F8:0A:DA:33:07:BA,0X1EFF4C00121910EC932CEEC3ED5D9A5BC697F417E838463EDBC55F99370136,0X121910EC932CEEC3ED5D9A5BC697F417E838463EDBC55F99370136,-23,-48,-55,-71,-77,0.461,1.201,2.723,4.109,5.164,Yes

107,0,F8:0A:DA:33:07:BA,0X1EFF4C00121910EC932CEEC3ED5D9A5BC697F417E838463EDBC55F9937014D,0X121910EC932CEEC3ED5D9A5BC697F417E838463EDBC55F9937014D,-22,-48,-56,-72,-76,0.412,1.989,3.082,2.978,5.011,Yes

108,0,F8:0A:DA:33:07:BA,0X1EFF4C00121910EC932CEEC3ED5D9A5BC697F417E838463EDBC55F9937014D,0X121910EC932CEEC3ED5D9A5BC697F417E838463EDBC55F9937014D,-24,-47,-56,-74,-83,0.416,1.432,2.745,4.115,7.734,Yes

109,0,F8:0A:DA:33:07:BA,0X1EFF4C00121910EC932CEEC3ED5D9A5BC697F417E838463EDBC55F9937014D,0X121910EC932CEEC3ED5D9A5BC697F417E838463EDBC55F9937014D,-28,-48,-60,-74,-83,0.234,1.077,1.314,4.804,4.379,Yes

110,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

111,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

112,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

113,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

114,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

115,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

116,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

117,0,E0:96:9E:0A:D5:15,0X1EFF4C001219103EF3CAC02A1E21566F92AA84CA730352231F1EA995CE0115,0X1219103EF3CAC02A1E21566F92AA84CA730352231F1EA995CE0115,-25,-47,-53,-72,-78,0.237,0.818,2.519,3.385,6.876,Yes

APPENDICES

118,0,E9:18:1C:C4:DF:D4,0X1EFF4C00121910E06D16E474A7B514F516B3E41E3F9F0F58E2926A28A701D4,0X121910E06D16E474A7B514F516B3E41E3F9F0F58E2926A28A701D4,-27,-46,-54,-70,-84,0.445,1.454,2.935,3.554,8.372,Yes

119,1,E0:96:9E:0A:D5:15,0X1EFF4C001219103EF3CAC02A1E21566F92AA84CA730352231F1EA995CE0115,0X1219103EF3CAC02A1E21566F92AA84CA730352231F1EA995CE0115,-25,-46,-55,-74,-76,0.373,1.748,2.533,3.605,6.832,Yes

120,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

121,0,E0:96:9E:0A:D5:15,0X1EFF4C001219103EF3CAC02A1E21566F92AA84CA730352231F1EA995CE01A9,0X1219103EF3CAC02A1E21566F92AA84CA730352231F1EA995CE01A9,-27,-49,-54,-74,NA,0.495,1.403,1.685,4.507,NA,Yes

122,0,E9:18:1C:C4:DF:D4,0X1EFF4C00121910E06D16E474A7B514F516B3E41E3F9F0F58E2926A28A70133,0X121910E06D16E474A7B514F516B3E41E3F9F0F58E2926A28A70133,-25,-46,-59,-73,NA,0.387,1.788,3.069,3.719,NA,Yes

123,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

124,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

125,0,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

126,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

127,0,FB:BE:01:49:CF30,0X1EFF4C001219102535C8163BF3FCB94EC444D8E596CCAB58DBAD8AC1030130,0X1219102535C8163BF3FCB94EC444D8E596CCAB58DBAD8AC1030130,-23,-48,-58,-73,NA,0.31,1.615,2.801,4.574,NA,Yes

128,0,FB:BE:01:49:CF30,0X1EFF4C001219102535C8163BF3FCB94EC444D8E596CCAB58DBAD8AC10301CD,0X1219102535C8163BF3FCB94EC444D8E596CCAB58DBAD8AC10301CD,-25,-46,-59,-71,NA,0.349,1.231,1.251,3.008,NA,Yes

129,0,FB:BE:01:49:CF30,0X1EFF4C001219102535C8163BF3FCB94EC444D8E596CCAB58DBAD8AC10301A8,0X1219102535C8163BF3FCB94EC444D8E596CCAB58DBAD8AC10301A8,-23,-45,-57,-70,NA,0.395,1.417,2.138,2.864,NA,Yes

130,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

APPENDICES

131,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

132,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

133,0,E3:85:FB:F3:B9:E1,0X1EFF4C00121910D2FC25FF3436B1E9447990806A050581C345
3369289603E1,0X121910D2FC25FF3436B1E9447990806A050581C3453369289603E1,-22,-
47,-52,-73,-81,0.251,1.578,1.472,2.129,6.714,Yes

134,0,E3:85:FB:F3:B9:E1,0X1EFF4C00121910D2FC25FF3436B1E9447990806A050581C345
336928960374,0X121910D2FC25FF3436B1E9447990806A050581C345336928960374,-28,-
48,-55,-71,-83,0.416,1.413,2.422,2.101,7.885,Yes

135,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

136,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

137,0,FF:E8:3B:14:1C:B8,0X1EFF4C0012191018DF0AD33AC75EF359AEE5CB3B70C9FDB
05D8E86EC7402B8,0X12191018DF0AD33AC75EF359AEE5CB3B70C9FDB05D8E86EC740
2B8,-26,-49,-63,-72,-79,0.495,1.99,2.415,2.943,7.705,Yes

138,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

139,0,C8:16:46:95:31:34,0X1EFF4C0012191094ACA0202747A0D03EE9D77C1DC12FEB137
08AC539B00034,0X12191094ACA0202747A0D03EE9D77C1DC12FEB13708AC539B00034,
-28,-48,-60,-70,-83,0.4,2.024,1.105,2.063,6.267,Yes

140,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

141,0,F8:C7:9E:74:68:97,0X1EFF4C001219109BF344DDFF66F6FA38BB12A264138D1E330
F75DA79FD0231,0X1219109BF344DDFF66F6FA38BB12A264138D1E330F75DA79FD0231,
-23,-45,-61,-70,-80,0.464,1.143,2.408,5.198,4.928,Yes

142,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

143,0,CB:7E:76:E6:C8:FE,0X1EFF4C00121910220D376736FD15B442C62F9D08A5DC8ABD
79B01A7CC20367,0X121910220D376736FD15B442C62F9D08A5DC8ABD79B01A7CC2036
7,-24,-45,-54,-71,NA,0.341,1.335,2.439,3.225,NA,Yes

144,1,NA,NA,NA,NA,NA,NA,NA,NA,,,,,,NA,No

APPENDICES

145,0,E5:84:13:7C:63:67,0X1EFF4C00121910A8A62498EEB950B7BD66494203B0BB891517509EECA10367,0X121910A8A62498EEB950B7BD66494203B0BB891517509EECA10367,-23,-47,-53,-72,NA,0.251,1.793,0.875,4.698,NA,Yes

146,1,NA,NA,NA,NA,NA,NA,NA,NA,,,,,,NA,No

147,0,D2:49:B6:F2:60:31,0X1EFF4C00121910A582A34C8E406A2B067F9B3EBA838C549129E8A8C87F0131,0X121910A582A34C8E406A2B067F9B3EBA838C549129E8A8C87F0131,-23,-49,-63,-74,NA,0.351,1.269,2.081,3.879,NA,Yes

148,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

149,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

150,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

151,0,F8:7A:33:CE:F4:6D,0X1EFF4C00121910E12AD489C479BBC90A6F15FE7B853C7866FF00E01BC456E9,0X121910E12AD489C479BBC90A6F15FE7B853C7866FF00E01BC456E9,-25,-45,-59,-73,NA,0.384,0.869,1.98,4.317,NA,Yes

152,0,F8:7A:33:CE:F4:6D,0X1EFF4C00121910E12AD489C479BBC90A6F15FE7B853C7866FF00E01BC456E9,0X121910E12AD489C479BBC90A6F15FE7B853C7866FF00E01BC456E9,-26,-45,-57,-73,NA,0.287,1.676,2.158,4.65,NA,Yes

153,0,F8:7A:33:CE:F4:6D,0X1EFF4C00121910E12AD489C479BBC90A6F15FE7B853C7866FF00E01BC45625,0X121910E12AD489C479BBC90A6F15FE7B853C7866FF00E01BC45625,-23,-48,-61,-73,NA,0.299,1.821,2.096,4.998,NA,Yes

154,0,F8:7A:33:CE:F4:6D,0X1EFF4C00121910E12AD489C479BBC90A6F15FE7B853C7866FF00E01BC45625,0X121910E12AD489C479BBC90A6F15FE7B853C7866FF00E01BC45625,-22,-49,-53,-72,NA,0.431,1.782,1.617,5.207,NA,Yes

155,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

156,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

157,0,E8:33:10:AB:1D:C0,0X1EFF4C00121910EE046A3C7D7899AA023C66CF93A170DD0BC626A72E0C34F3,0X121910EE046A3C7D7899AA023C66CF93A170DD0BC626A72E0C34F3,-27,-47,-56,-73,-76,0.408,0.983,2.399,3.288,6.101,Yes

APPENDICES

158,0,E8:33:10:AB:1D:C0,0X1EFF4C00121910EE046A3C7D7899AA023C66CF93A170DD0BC626A72E0C34BC,0X121910EE046A3C7D7899AA023C66CF93A170DD0BC626A72E0C34BC,-22,-49,-58,-71,-84,0.292,0.912,1.512,2.713,7.985,Yes

159,0,E8:33:10:AB:1D:C0,0X1EFF4C00121910EE046A3C7D7899AA023C66CF93A170DD0BC626A72E0C348F,0X121910EE046A3C7D7899AA023C66CF93A170DD0BC626A72E0C348F,-24,-48,-58,-71,-78,0.308,1.06,2.976,3.728,7.615,Yes

160,0,CB:05:67:BE:F2:9D,0X1EFF4C001219100F162733EB284CA0084AF8231184D0638CAA24511BE609BA,0X1219100F162733EB284CA0084AF8231184D0638CAA24511BE609BA,-27,-49,-63,-70,-83,0.261,0.806,0.991,3.923,6.593,Yes

161,0,CB:05:67:BE:F2:9D,0X1EFF4C001219100F162733EB284CA0084AF8231184D0638CAA24511BE6094E,0X1219100F162733EB284CA0084AF8231184D0638CAA24511BE6094E,-27,-47,-61,-72,-83,0.227,1.702,1.872,5.019,5.965,Yes

162,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

163,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

164,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

165,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

166,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

167,0,E6:97:D6:BA:C3:DA,0X1EFF4C0012191060D6C2598EA86EDAE003AAB5C16079E5252E6EE4711B03DA,0X12191060D6C2598EA86EDAE003AAB5C16079E5252E6EE4711B03DA,-28,-48,-63,-73,-79,0.382,0.938,2.861,4.398,4.904,Yes

168,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

169,0,D8:20:1C:20:C1:E0,0X1EFF4C001219104D594D225A97D273C243B8AFD5B1E7F9CA339502606B00E0,0X1219104D594D225A97D273C243B8AFD5B1E7F9CA339502606B00E0,-25,-49,-63,-70,-83,0.247,1.37,1.264,3.798,7.888,Yes

170,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

APPENDICES

171,0,F9:65:74:41:91:D7,0X1EFF4C00121910C7CE58F34DF045A16246FA3C53AF0DE2A08A81AF037B00D7,0X121910C7CE58F34DF045A16246FA3C53AF0DE2A08A81AF037B00D7,-22,-47,-58,-73,-79,0.444,1.93,1.69,3.169,6.104,Yes

172,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

173,0,D7:CC:14:52:F6:02,0X1EFF4C001219109044C9A1694A8D6AB15CA336A625715E3EF7651007240002,0X1219109044C9A1694A8D6AB15CA336A625715E3EF7651007240002,-23,-47,-55,-73,-81,0.349,0.814,2.705,2.073,6.91,Yes

174,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

175,0,CC:35:4C:9A:AB:F6,0X1EFF4C0012191082A7CD6D1FBE3DC51981405FE6D9B42D7137A44990BA03F6,0X12191082A7CD6D1FBE3DC51981405FE6D9B42D7137A44990BA03F6,-22,-46,-53,-73,-80,0.34,0.854,2.996,2.628,5.446,Yes

176,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

177,0,FB:EF:04:1E:AC:07,0X1EFF4C00121910A5C82371BB79D3026452271A146109E4837526BABCEE0107,0X121910A5C82371BB79D3026452271A146109E4837526BABCEE0107,-23,-48,-54,-74,-84,0.26,1.433,2.117,4.161,6.302,Yes

178,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

179,0,E6:75:20:25:D3:6C,0X1EFF4C00121910CE3308BA50FF12CA587EF3370A8E0B1170DD2AA8B10552C3,0X121910CE3308BA50FF12CA587EF3370A8E0B1170DD2AA8B10552C3,-25,-45,-60,-71,-82,0.393,1.941,1.584,3.666,4.343,Yes

180,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

181,0,D8:14:55:3A:F7:63,0X1EFF4C00121910C7200AF77317EE0C85BBA232011EF0BA653309A8CA104D6D,0X121910C7200AF77317EE0C85BBA232011EF0BA653309A8CA104D6D,-25,-49,-52,-74,-80,0.469,0.866,2.226,3.901,4.553,Yes

182,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

183,0,EC:48:8A:A6:98:6B,0X1EFF4C00121910660BC0E7D5A7C294EA52FFF0797124A8BC71BADAE062006B,0X121910660BC0E7D5A7C294EA52FFF0797124A8BC71BADAE062006B,-27,-45,-53,-74,-76,0.361,1.644,3.113,5.098,4.224,Yes

APPENDICES

184,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

185,0,E3:1F:F8:5D:1B:EB,0X1EFF4C00121910967F20B53E7EC60496511C3E5CCD50200B9E989E65C802EB,0X121910967F20B53E7EC60496511C3E5CCD50200B9E989E65C802EB,-25,-47,-56,-72,-79,0.323,1.599,1.095,4.023,6.714,Yes

186,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

187,0,E6:31:E8:A1:2B:7A,0X1EFF4C0012191031345CE0A87400ECD2055A47C944AB8BB385EA11DE259A0B,0X12191031345CE0A87400ECD2055A47C944AB8BB385EA11DE259A0B,-24,-47,-53,-71,NA,0.447,1.668,1.381,5.26,NA,Yes

188,0,E6:31:E8:A1:2B:7A,0X1EFF4C0012191031345CE0A87400ECD2055A47C944AB8BB385EA11DE259A34,0X12191031345CE0A87400ECD2055A47C944AB8BB385EA11DE259A34,-27,-45,-54,-70,NA,0.262,1.196,3.06,4.289,NA,Yes

189,0,E6:31:E8:A1:2B:7A,0X1EFF4C0012191031345CE0A87400ECD2055A47C944AB8BB385EA11DE259A2F,0X12191031345CE0A87400ECD2055A47C944AB8BB385EA11DE259A2F,-25,-47,-60,-74,NA,0.467,1.391,1.925,3.742,NA,Yes

190,0,D3:E5:34:22:AC:8D,0X1EFF4C00121910EB300356A85EDE281F7FA0355A6EBD88DF1608244A6EBC2D,0X121910EB300356A85EDE281F7FA0355A6EBD88DF1608244A6EBC2D,-23,-46,-52,-71,NA,0.265,1.295,1.162,3.596,NA,Yes

191,0,D3:E5:34:22:AC:8D,0X1EFF4C00121910EB300356A85EDE281F7FA0355A6EBD88DF1608244A6EBCA8,0X121910EB300356A85EDE281F7FA0355A6EBD88DF1608244A6EBCA8,-23,-47,-59,-73,NA,0.416,1.708,2.97,5.273,NA,Yes

192,0,D3:E5:34:22:AC:8D,0X1EFF4C00121910EB300356A85EDE281F7FA0355A6EBD88DF1608244A6EBC7C,0X121910EB300356A85EDE281F7FA0355A6EBD88DF1608244A6EBC7C,-23,-46,-56,-74,NA,0.369,1.502,2.063,2.976,NA,Yes

193,0,F5:2A:32:EB:45:87,0X1EFF4C001219107AA23EF87065011EAAC69704AFCB348BEE1A9CFF740400AC,0X1219107AA23EF87065011EAAC69704AFCB348BEE1A9CFF740400AC,-24,-45,-61,-73,-78,0.474,1.381,2.591,4.919,8.459,Yes

APPENDICES

194,0,F5:2A:32:EB:45:87,0X1EFF4C001219107AA23EF87065011EAAC69704AFCB348BEE1A9CFF74040056,0X1219107AA23EF87065011EAAC69704AFCB348BEE1A9CFF74040056,-27,-45,-62,-73,-79,0.462,0.791,0.894,4.395,6.667,Yes

195,0,C9:AE:3F:66:82:A1,0X1EFF4C00121910E9FAA31336CAFB54070E07255EA6288AB0F7EE226A660A22,0X121910E9FAA31336CAFB54070E07255EA6288AB0F7EE226A660A22,-23,-48,-58,-71,-76,0.494,1.301,1.662,4.301,7.447,Yes

196,0,C9:AE:3F:66:82:A1,0X1EFF4C00121910E9FAA31336CAFB54070E07255EA6288AB0F7EE226A660AE8,0X121910E9FAA31336CAFB54070E07255EA6288AB0F7EE226A660AE8,-24,-46,-55,-71,-76,0.359,1.111,2.824,2.612,7.814,Yes

197,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

198,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

199,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

200,1,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,NA,No

APPENDICES

Signal Strength for BLE Devices

Results for Signal Strength(dBm) at 0°

Distances(m)	0.02	0.10	0.25	0.50	0.75	1.00	1.50	2.00	2.50	3.00	5.00	7.00	10.00
AirTag	-21	-35	-45	-49	-57	-63	-64	-63	-74	-71	-79	-79	-80
Laptop	-27	-33	-36	-45	-52	-65	-61	-63	-65	-70	-81	-79	-83
iPhone	-30	-32	-38	-48	-50	-52	-56	-62	-63	-69	-75	-81	-79

Results for Signal Strength(dBm) at 90°

Distances(m)	0.02	0.10	0.25	0.50	0.75	1.00	1.50	2.00	2.50	3.00	5.00	7.00	10.00
AirTag	-23	-44	-47	-48	-48	-52	-60	-61	-68	-70	-76	-79	-82
Laptop	21	-26	-33	-44	-54	-56	-58	-60	-60	-62	-70	-74	-75
iPhone	21	-29	-36	-49	-48	-51	-55	-59	-66	-70	-79	-76	-77

Results for Signal Strength(dBm) at 180°

Distances(m)	0.02	0.10	0.25	0.50	0.75	1.00	1.50	2.00	2.50	3.00	5.00	7.00	10.00
AirTag	-34	-42	-44	-47	-48	-59	-66	-68	-79	-75	-84	-92	-90
Laptop	-35	-38	-48	-47	-49	-63	-71	-73	-80	-83	-87	-90	-91
iPhone	-23	-29	-42	-46	-57	-59	-62	-65	-72	-77	-80	-86	-90

Results for Signal Strength(dBm) at 270°

Distances(m)	0.02	0.10	0.25	0.50	0.75	1.00	1.50	2.00	2.50	3.00	5.00	7.00	10.00
AirTag	-27	-38	-48	-56	-59	-60	-64	-69	-67	-73	-82	-77	-83
Laptop	-23	-38	-49	-57	-57	-59	-63	-69	-64	-73	-75	-71	-76
iPhone	-30	-33	-47	-51	-59	-63	-62	-70	-74	-77	-83	-85	-80

APPENDICES

Machine Learning Algorithm Evaluation Results

Naïve Bayes

Correctly **Classified Instances – 197 – 98.5%**

Incorrectly Classified Instances – 3 – 1.5 %

Kappa Statistic – 0.97

Mean Absolute Error – 0.0151

Root Mean Squared Error – 0.1207

Relative Absolute Error – 3.026 %

Root Relative Squared Error – 24.136 %

Total Number of Instances – 200

Cross-Validation Folds - 10

Detailed Accuracy Metrics by Class

	TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	PRC Area	Class
	0.971	0.000	1.000	0.971	0.985	0.970	0.991	0.995	Yes
	1.000	0.029	0.970	1.000	0.985	0.970	0.991	0.976	No
AVG	0.985	0.014	0.985	0.985	0.985	0.970	0.991	0.986	

Confusion Matrix

A	b	Classified as
99	3	a=Yes
0	98	B=No

APPENDICES

Support Vector Machine

Correctly Classified Instances – 199 – 99.5%

Incorrectly Classified Instances – 1 – 0.5 %

Kappa Statistic – 0.99

Mean Absolute Error – 0.005

Root Mean Squared Error – 0.0707

Relative Absolute Error – 1.0002 %

Root Relative Squared Error – 14.1423 %

Total Number of Instances – 200

Cross-Validation Folds - 10

Detailed Accuracy Metrics by Class

	TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	PRC Area	Class
	0.990	0.000	1.000	0.991	0.995	0.990	0.995	0.995	Yes
	1.000	0.010	0.990	1.000	0.995	0.990	0.995	0.990	No
AVG	0.995	0.005	0.995	0.995	0.995	0.990	0.995	0.993	

Confusion Matrix

A	b	Classified as
101	1	a=Yes
0	98	B=No

APPENDICES

Random Forest

Correctly Classified Instances – 199 – 99.5%

Incorrectly Classified Instances – 1 – 0.5 %

Kappa Statistic – 0.99

Mean Absolute Error – 0.1221

Root Mean Squared Error – 0.2058

Relative Absolute Error – 24.4289 %

Root Relative Squared Error – 41.1512 %

Total Number of Instances – 200

Cross-Validation Folds - 10

Detailed Accuracy Metrics by Class

	TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	PRC Area	Class
	0.990	0.000	1.000	0.991	0.995	0.990	0.995	0.995	Yes
	1.000	0.010	0.990	1.000	0.995	0.990	0.995	0.989	No
AVG	0.995	0.005	0.995	0.995	0.995	0.990	0.995	0.992	

Confusion Matrix

A	b	Classified as
101	1	a=Yes
0	98	B=No

Appendix C

Overall Codes

APPENDICES

Linear Regression Model Construction and Validation

Linear Regression Model

```
import pandas as pd

import numpy as np

import matplotlib.pyplot as plt

signal_strength = pd.read_csv("D:\Desktop\MSC\DISSERTATION\signal strength experiment.csv")


from statsmodels.formula.api import ols

model = ols('rssi ~ distance', data=signal_strength).fit()

print(model.params)


from sklearn.linear_model import LinearRegression

model1 = LinearRegression()

model1.fit(signal_strength[['distance']],signal_strength['rssi'])

print('intercept:', model1.intercept_)

print('slope:', model1.coef_)
```

Line of best Fit

```
plt.plot(signal_strength['distance'], signal_strength['rssi'], 'o')

plt.plot(signal_strength['distance'], model1.coef_*signal_strength['distance'] + model1.intercept_)

plt.title("Fitting line plot")

plt.xlabel("Distance in m")
```

APPENDICES

```
plt.ylabel("Signal Strength in dBm")

plt.show()
```

Residual Plot

```
import statsmodels.api as sm

fig = plt.figure(figsize=(12,8))

#produce regression plots

fig = sm.graphics.plot_regress_exog(model, 'distance', fig=fig)
```

Coefficient of Determination

```
import numpy as np

correlation_matrix = np.corrcoef(signal_strength['distance'],  signal_strength['rssi'])

correlation_xy = correlation_matrix[0,1]

r_squared = correlation_xy**2

print(r_squared)
```

APPENDICES

Kotlin Implementation

MainActivity

```
package com.example.airtagantistalker


import android.Manifest
import android.app.Activity
import android.app.NotificationChannel
import android.app.NotificationManager
import android.app.PendingIntent
import android.bluetooth.BluetoothAdapter
import android.bluetooth.BluetoothDevice
import android.bluetooth.BluetoothManager
import android.bluetooth.le.ScanCallback
import android.bluetooth.le.ScanFilter
import android.bluetooth.le.ScanResult
import android.bluetooth.le.ScanSettings
import android.content.Context
import android.content.Intent
import android.content.pm.PackageManager
import android.graphics.BitmapFactory
import android.os.Build
import android.os.Bundle
import android.os.CountDownTimer
import androidx.appcompat.app.AppCompatActivity
import androidx.core.app.ActivityCompat
import androidx.core.app.NotificationCompat
import androidx.core.app.NotificationManagerCompat
import androidx.core.content.ContextCompat
import androidx.recyclerview.widget.LinearLayoutManager
import androidx.recyclerview.widget.RecyclerView
import androidx.recyclerview.widget.SimpleItemAnimator
import kotlinx.android.synthetic.main.activity_main.scan_button
import kotlinx.android.synthetic.main.activity_main.scan_results_recycler_view
```

APPENDICES

```
import kotlinx.android.synthetic.main.row_scan_result.timer
import org.jetbrains.anko.alert
import org.jetbrains.anko.appcompatV7.BuildConfig
import timber.log.Timber

private const val ENABLE_BLUETOOTH_REQUEST_CODE = 1
private const val LOCATION_PERMISSION_REQUEST_CODE = 2

class MainActivity : AppCompatActivity() {



    private val bluetoothAdapter: BluetoothAdapter by lazy {
        val bluetoothManager = getSystemService(BLUETOOTH_SERVICE) as
BluetoothManager
        bluetoothManager.adapter
    }

    private val airTagScanner by lazy {
        bluetoothAdapter.bluetoothLeScanner
    }



    /*scan settings for the application using low power scan mode */
    private val scanSettings = ScanSettings.Builder()
        .setScanMode(ScanSettings.SCAN_MODE_LOW_LATENCY)
        .build()

    private var isScanning = false
        set(value) {
            field = value
            runOnUiThread { scan_button.text = if (value) "Stop AirTag
Tracking" else "Search for AirTags" }
        }
```

APPENDICES

```
    private val scanResults = mutableListOf<ScanResult>()
    private val scanResultAdapter: ScanResultAdapter by lazy {
        ScanResultAdapter(scanResults) { result ->
            if (isScanning) {
                stopAirTagScan()
            }

        }
    }

    private val isLocationPermissionGranted
        get() = hasPermission(Manifest.permission.ACCESS_FINE_LOCATION)




    override fun onCreate(savedInstanceState: Bundle?) {
        super.onCreate(savedInstanceState)
        setContentView(R.layout.activity_main)
        if (BuildConfig.DEBUG) {
            Timber.plant(Timber.DebugTree())
        }
        scan_button.setOnClickListener { if (isScanning) stopAirTagScan() else
startAirTagScan() }
        setupRecyclerView()
        createNotificationChannel()
    }


    override fun onResume() {
        super.onResume()


        if (!bluetoothAdapter.isEnabled) {
            promptEnableBluetooth()
        }
    }
```

APPENDICES

```
    override fun onActivityResult(requestCode: Int, resultCode: Int, data:
Intent?) {
        super.onActivityResult(requestCode, resultCode, data)
        when (requestCode) {
            ENABLE_BLUETOOTH_REQUEST_CODE -> {
                if (resultCode != RESULT_OK) {
                    promptEnableBluetooth()
                }
            }
        }
    }


    override fun onRequestPermissionsResult(
        requestCode: Int,
        permissions: Array<out String>,
        grantResults: IntArray
    ) {
        super.onRequestPermissionsResult(requestCode,             permissions,
grantResults)
        when (requestCode) {
            LOCATION_PERMISSION_REQUEST_CODE -> {
                if               (grantResults.firstOrNull()               ==
PackageManager.PERMISSION_DENIED) {
                    requestLocationPermission()
                } else {
                    startAirTagScan()
                }
            }
        }
    }


    /*implemntation of scan filter using Identifying Token (0x12, 0x19, 0x10)
in decimal form
           They are parsed into ByteArray form to be used by the filter */
```

APPENDICES

```
    fun byteArrayOfInts(vararg ints: Int) = ByteArray(ints.size) { pos ->
ints[pos].toByte() }


    private val airtagManData = byteArrayOfInts(18, 25, 16)


    private val filter1 = ScanFilter.Builder().setManufacturerData(
        76, airtagManData
    ).build()


    /* The filter build is then added to the Filter List*/
    private val devfilters : MutableList<ScanFilter> = ArrayList()




    /*alert system for application using Notification System */
    //Notification Channel Creation
    private val CHANNEL_ID = "airtag_detected"
    private val notificationId = 101


    private fun createNotificationChannel() {
        // Create the NotificationChannel, but for only API 26+ because
        // the NotificationChannel class is new and not in the support library
        if (Build.VERSION.SDK_INT >= Build.VERSION_CODES.O) {
            val name = "AirTag Detection Alert"
            val descriptionText = "Notifies when a potential detected airTag is
stalking"
            val importance = NotificationManager.IMPORTANCE_HIGH
            val    channel    =    NotificationChannel(CHANNEL_ID,    name,
importance).apply {
                description = descriptionText
            }
            // Registering the channel with the system
            val notificationManager: NotificationManager =
                getSystemService(Context.NOTIFICATION_SERVICE)              as
NotificationManager
```

APPENDICES

```
            notificationManager.createNotificationChannel(channel)
        }
    }

    //function for sending notification alert with High Priority
    private fun sendNotification(){
        val intent = Intent(this, MainActivity::class.java).apply{
            flags = Intent.FLAG_ACTIVITY_NEW_TASK or
Intent.FLAG_ACTIVITY_CLEAR_TASK
        }

        val pendingIntent: PendingIntent = PendingIntent.getActivity(this, 0,
intent, 0)

        val bitmap =
BitmapFactory.decodeResource(applicationContext.resources,
R.drawable.apple_airtag)

        val builder = NotificationCompat.Builder(this, CHANNEL_ID)
            .setSmallIcon(R.drawable.apple_airtag)
            .setContentTitle("AIRTAG DETECTED!!")
            .setContentText("Potential Stalking by AirTag!!!")
            .setLargeIcon(bitmap)
            .setContentIntent(pendingIntent)
            .setPriority(NotificationCompat.PRIORITY_HIGH)

        with(NotificationManagerCompat.from(this)){
            notify(notificationId, builder.build())
        }
    }


    //Timer implementation before a notification alert is given, set to 1 minute
    lateinit var alert_timer: CountDownTimer
    var isRunning: Boolean = false;
```

APPENDICES

```
    var time_in_milli_seconds = 0L

    private fun startTimer(time_in_seconds: Long) {
        alert_timer = object : CountDownTimer(time_in_seconds, 1000) {
            override fun onFinish() {
                sendNotification()
            }

            override fun onTick(p0: Long) {
                time_in_milli_seconds = p0
                updateTimerText()
            }
        }
        alert_timer.start()

        isRunning = true

    }

    private fun updateTimerText() {
        val mins = (time_in_milli_seconds / 1000) / 60
        val secs = (time_in_milli_seconds / 1000) % 60

        timer.text = "$mins:$secs"
    }




    /*prompts for Bluetooth to be enabled on device*/
    private fun promptEnableBluetooth() {
       if (!bluetoothAdapter.isEnabled) {
            val                         enableBtIntent                         =
Intent(BluetoothAdapter.ACTION_REQUEST_ENABLE)
```

APPENDICES

```
            startActivityForResult(enableBtIntent,
ENABLE_BLUETOOTH_REQUEST_CODE)
        }
    }

    /*performs AirTag Scanning Process using filter and scan settings*/
    private fun startAirTagScan() {
        if     (Build.VERSION.SDK_INT     >=     Build.VERSION_CODES.M     &&
!isLocationPermissionGranted) {
            requestLocationPermission()
        } else {
            scanResults.clear()
            scanResultAdapter.notifyDataSetChanged()
            devfilters.add(filter1)
            airTagScanner.startScan(devfilters, scanSettings, scanCallback)
            isScanning = true
        }
    }

    /*stops the AirTag scanning process*/
    private fun stopAirTagScan() {
        airTagScanner.stopScan(scanCallback)
        isScanning = false
    }

    /* used to request for location as a requirement for using Bluetooth in
Android*/
    private fun requestLocationPermission() {
        if (isLocationPermissionGranted) {
            return
        }
        runOnUiThread {
            alert {
                title = "Location permission required"
```

APPENDICES

```
                message = "Starting from Android M (6.0), the system requires
apps to be granted " +
                    "location access in order to search for AirTags."
                isCancelable = false
                positiveButton(android.R.string.ok) {
                    requestPermission(
                        Manifest.permission.ACCESS_FINE_LOCATION,
                        LOCATION_PERMISSION_REQUEST_CODE
                    )
                }
            }.show()
        }
    }

    private fun setupRecyclerView() {
        scan_results_recycler_view.apply {
            adapter = scanResultAdapter
            layoutManager = LinearLayoutManager(
                this@MainActivity,
                RecyclerView.VERTICAL,
                false
            )
            isNestedScrollingEnabled = false
        }

        val animator = scan_results_recycler_view.itemAnimator
        if (animator is SimpleItemAnimator) {
            animator.supportsChangeAnimations = false
        }
    }

    /* Scan Result Callbacks */
    private val scanCallback = object : ScanCallback() {
        override fun onScanResult(callbackType: Int, result: ScanResult) {
```

APPENDICES

```
            val indexQuery = scanResults.indexOfFirst { it.device.address == result.device.address }
            if (indexQuery != -1) { // A scan result already exists with the same address
                scanResults[indexQuery] = result
                scanResultAdapter.notifyItemChanged(indexQuery)
            } else {
                with(result.device) {
                    Timber.i("Found BLE device! Name: ${name ?: "Unnamed"}, address: $address")
                }
                scanResults.add(result)
                scanResultAdapter.notifyItemInserted(scanResults.size - 1)
                startTimer(60000)
            }
        }

        override fun onScanFailed(errorCode: Int) {
            Timber.e("onScanFailed: code $errorCode")
        }
    }



    /*permission extenction functions */
    private fun Context.hasPermission(permissionType: String): Boolean {
        return ContextCompat.checkSelfPermission(this, permissionType) ==
            PackageManager.PERMISSION_GRANTED
    }

    private fun Activity.requestPermission(permission: String, requestCode: Int) {
        ActivityCompat.requestPermissions(this, arrayOf(permission), requestCode)
    }
```

APPENDICES

```
}
```

ScanResultsAdapter

```
package com.example.airtagantistalker


import android.bluetooth.le.ScanResult

import android.view.View

import android.view.ViewGroup

import androidx.recyclerview.widget.RecyclerView

import kotlinx.android.synthetic.main.row_scan_result.view.device_name

import kotlinx.android.synthetic.main.row_scan_result.view.estimatedDistance

import kotlinx.android.synthetic.main.row_scan_result.view.mac_address

import kotlinx.android.synthetic.main.row_scan_result.view.signal_strength

import
kotlinx.android.synthetic.main.row_scan_result.view.manufacturer_specific_dat
a

import org.jetbrains.anko.layoutInflater

import java.math.BigDecimal

import java.math.RoundingMode

import kotlin.math.pow


class ScanResultAdapter(

    private val items: List<ScanResult>,

    private val onClickListener: ((device: ScanResult) -> Unit)

) : RecyclerView.Adapter<ScanResultAdapter.ViewHolder>() {


    override fun onCreateViewHolder(parent: ViewGroup, viewType: Int):
ViewHolder {

        val view = parent.context.layoutInflater.inflate(

            R.layout.row_scan_result,

            parent,

            false

        )

        return ViewHolder(view, onClickListener)

    }
```

APPENDICES

```
    override fun getItemCount() = items.size

    override fun onBindViewHolder(holder: ViewHolder, position: Int) {
        val item = items[position]
        holder.bind(item)
    }

    class ViewHolder(
        private val view: View,
        private val onClickListener: ((device: ScanResult) -> Unit)
    ) : RecyclerView.ViewHolder(view) {

        /* parser to convert from ByteArray to string */
        private val HEX = "0123456789ABCDEF".toCharArray()
        fun toHexString(bytes: ByteArray): String {
            if (bytes.isEmpty()) {
                return ""
            }
            val hexChars = CharArray(bytes.size * 2)
            for (j in bytes.indices) {
                val v = (bytes[j].toInt() and 0xFF)
                hexChars[j * 2] = HEX[v ushr 4]
                hexChars[j * 2 + 1] = HEX[v and 0x0F]
            }
            return String(hexChars)
        }

        fun bind(result: ScanResult) {

            /*parsing the Manufacturer Specific Data(MSD) of AirTag into
readable format*/
            var logtimber: String = "hello"
```

APPENDICES

```
            val                    airtagManufacturerData                    =
result.scanRecord?.getManufacturerSpecificData(76)
            if (airtagManufacturerData != null) {
                val parsedMSD = toHexString(airtagManufacturerData)

                logtimber = "Manufacturer Specific Data:$parsedMSD "
            }

        //calculating estimated distance using Measured Power of -53.4 dBm and
N=4.5
            val eXP: Double  = ((-53.4-(result.rssi))/45)
            val distanceEstimateLong: Double = 10.0.pow(eXP)
            val                        distanceEstimate                        =
BigDecimal(distanceEstimateLong).setScale(2, RoundingMode.HALF_EVEN)

        //displaying scan results of devices after scanning such as  MAC
Address, RSSI,
            // MSD and estimated distance
            view.device_name.text = result.device.name ?: "Unnamed"
            view.mac_address.text = result.device.address
            view.manufacturer_specific_data.text = logtimber
            view.signal_strength.text = "${result.rssi} dBm"
            view.estimatedDistance.text = "${distanceEstimate.toString()} m"
            view.setOnClickListener { onClickListener.invoke(result) }
        }
    }
}
```